SPECIFICATION GUIDE

DSX Access Systems, Inc.
10731 Rockwall Road
Dallas, Texas 75238
(214) 553-6140 voice
(214) 553-6147 facsimile
(888) 419-8353 voice
http:/www.dsxinc.com
Email: sales@dsxinc.com

SECTION 28 10 00
ELECTRONIC ACCESS CONTROL/INTRUSION DETECTION

****

Welcome to the DSX System Specification Guide! DSX Access Systems has prepared this specification guide in printed and electronic media, as an aid to specifics in preparing written construction documents for a PC based Building/Facility Management and Monitoring System. The DSX solution is Multi-user, Multi-tasking system that integrates access control, alarm monitoring, CCTV control, DVR integration, elevator control, HVAC control, guard tour, time and attendance, and video imaging into a single Windows application.

Edit entire Master to suit project requirements. Modify or add items as necessary. Delete items that are not applicable. Words and sentences within brackets [_____] reflect a choice to be made regarding inclusion or exclusion of a particular item or statement. This section may include performance, proprietary and descriptive type specifications. Edit to avoid conflicting requirements. Editor notes to guide the specified are included between lines of asterisks to assist in choices to be made.

This guide specification is based on the Construction Specifications Institute (CSI), Section Format standards, and references to section names and numbers are based on CSI Master Format 2004.

For specification assistance on specific product applications, please contact the offices above.

DSX Access Systems Inc., reserves the right to modify these guide specifications at any time. Updates to this guide specification will be posted as they occur. DSX Access Systems Inc. makes no expressed or implied warranties regarding content, errors, or omissions in the information presented. Specifications modified or rewritten in excess of manufacturer's standard process, products, and procedures may void warranties and related remedies.

****

GENERAL

1.1 SUMMARY

A. Related Documents: Provisions established within the General and Supplementary Conditions of the Contract, Division 1 - General Requirements and the Drawings are collectively applicable to this Section.

B. Section Includes:

****

Edit the "Section Includes" paragraph to briefly describe the content of the section. After editing section, refer back to this paragraph to verify no conflicts occur.

****

1. Complete access control and alarm monitoring for sites indicated, including:
   a) Access control.
   b) Security:
      1) [Threat Level Management]
      2) [Time Zones controlled with Linking Logic]
      3) [Virtual Outputs]
      4) [First Man In Rule]
      5) [Manager First Rule]
      6) [Two Man Rule]
      7) [Hazmat Lockdown]
      8) [Hot-Swap Communications Server]
      9) [Point Monitoring.]
      10) [High Level Elevator Control Interface.]
      11) [Photo ID Badging.]
      12) [Guard Tour.]
      13) [Time and Attendance.]
      14) [Key Tracking.]
      15) [Image Recall with Historic and User Accountability Reporting.]
      16) [Live CCTV display/control.]
      17) [Interface with Paging, CCTV, Parking, Central Station Automated Alarm Systems, HVAC, and Elevator Control Systems.]
      18) [Digital Video Recorder Integration]
      19) [AES-256bit Encryption between the communication server and the field controllers and between communication server and workstations.]
      20) [Integrated functions for seamless biometric enrollment for Integrated Biometrics finger print readers.]

C. Related Sections:
   1. Section 28 16 00 - Monitoring and Access Control Hardware.

****

Below section “System Overview” is informational only and may be included or excluded depending on project.

****

SYSTEM OVERVIEW

D. PC based: The system is a PC based Building/Facility Management and Monitoring System used to control and monitor personnel and alarm activity. The DSX system provides 5 different controllers that offer various configurations of card reader inputs, relay outputs and alarm inputs. These controllers can be combined to provide the exact number of inputs and outputs required for each application. DSX controllers use fully distributed database architecture with real-time processing performed at each controller.

E. Distributed Processing: This fully distributed processing provides that all information (time, date, valid codes, access levels, etc) is downloaded to the controllers so that each controller makes its own access control decisions. There are no hierarchical or intermediate processors to make decisions for the controllers. Also the PC is not required to make any decisions for the controllers including any global functions. This provides Instant response to card reads regardless of system size. This also provides for no degradation of system performance in the event of communication loss to the host (or

actual loss of host). All time zones, access levels, linking events, holiday schedules, and global functions remain operational. Upon communication loss to the host all controllers shall automatically buffer event transactions until the host communications is restored, at which time the buffered events will be automatically uploaded to the host. The system maintains full feature capability regardless of the style of the communications from the PC. This means that DSX dial-up modem sites can utilize all standard features like elevator control and linking between controllers without the PC needing to be online.

F. System Size: The system is designed to support up to 32,000 separate Locations using a single PC with combinations of direct connect, dial-up or TCP/IP LAN connections to each Location. DSX defines a loop of up to 64 controllers as one Location. Each Location has its own database and history at the host PC. Locations may be combined to share a common database and create a very large network of controllers. Each Location can have up to 128 devices.

G. Intelligent Controllers: Each DSX controller is an Intelligent Control Unit. The first controller of every Location is designated as the "Master". All subsequent controllers at the same Location are designated as "Slaves". Any DSX controller may be selected by dipswitch settings to work as the Master controller. The Master controller performs all the same functions as a Slave controller, but it is also responsible for polling all Slave controllers and communicating with the host PC. The Master controller does not make any access decisions for the Slave controllers. It is simply the messenger for information from the controllers to the PC and for information from the PC to the controllers.

H. Controller operating system resides in Flash ROM on each controller. It is upgradeable thru a download from the Host PC to each of the 1040 Series and 1022 controllers in the system. Upgrades in controller operating system shall NOT require PROM changes.

I. Processing Power: Each intelligent controller uses an Intel microprocessor (same as a PC) as its engine. In a large system, the total processing may approach, or even exceed that of a Mini Computer. Instead of all the processing power being centralized in one "Mini" it is distributed throughout the system.

1.2 SYSTEM REQUIREMENTS

A. Software Requirements:

1. WinDSX is compatible with XP Pro Svc Pack 2, Windows Vista Business Svc Pack 1, Windows 7 Pro 32/64 bit, Windows 8 Pro 32/64 bit. Server platforms include Server 2000, 2003, 2008, and 2008 R2.
2. WinDSX-SQL program utilizes Microsoft SQL Server 2005 Svc Pack 3 /2008 ™
3. 2008 R2, and SQL 2012 for database deployment and management.
4. Multi-user and multi-tasking capability allowing for independent activities and monitoring to occur simultaneously at different Workstation PCs.
5. Utilize graphical user interface with simple pull-down menus and a menu tree format that conform to interface guidelines defined by Microsoft Corporation.
6. Allow for language localization.
7. Allow LAN/WAN network applications, using TCP/IP protocol, with up to 1000 Workstation PCs.
8. System shall be site licensed, not seat licensed.
9. System shall have open architecture that allows importing and exporting of data and ability to interface with other systems.
10. Operator Identification logon password protected.

B. Hardware Requirements:

1. Comm Server PC: Windows XP Pro, Vista Business, Windows 7 Pro, or Windows 8 Pro - PC with a 2.8 GHz Pentium processor / 2GB RAM (minimum) or greater depending on system scope. Server 2003, and 2008/R2 will work but not required.
2. Workstation PC: Windows XP Pro, Vista Business, Windows 7, Windows 8 Professional PC with a 2.8 GHz Pentium processor / 2GB RAM (minimum) or greater depending on system scope.
3. Other requirements as indicated herein.

1.3 QUALITY ASSURANCE

****

Include quality assurance requirements (below), which are consistent with the size and scope of the project and extent of work of this section. Only request qualification statements you intend to review, and which are necessary to establish qualifications of the product, manufacturer, or installer.

****

A. Manufacturer:

1. Minimum of 10 years experienced in providing security access control components for projects of similar nature and complexity.
2. Maintain a 24-hour toll free telephone assistance line for installing dealer support.

B. Installer:
   1. Minimum of 5 years experience in performing work of this section who has specialized in the installation of work similar to that required for this project.
   2. Have at least one technician trained by the manufacturer.
   3. Maintain adequate supply of replacement parts for system components provided.

C. Regulatory Requirements: Installed products shall meet standards of a recognized testing laboratory (UL. or comparable).

****

Include submittal requirements below that are consistent with the scope of the project and extent of work of this section. Only request those submittals that are necessary for review of design intent.

****

1.4 SUBMITTALS

A. Submit in accordance with requirements of Section 01 33 00.

B. Shop Drawings: Detailing all connected devices, of sufficient detail to adequately communicate that recommended software meets access system requirements, including:
   1. System device locations on architectural floor plans.
   2. Full schematic wiring information for all devices. Wiring information shall include cable type, conductor routings, quantities, and connection details at devices.
   3. A complete access control system one-line block diagram.
   4. System sequence operation description.

C. Product Data:
   1. Manufacturer’s data for all material and equipment, including terminal devices, local processors, computer equipment, access cards, and any other equipment required for the complete access management and alarm monitoring system.
   2. System description, including analysis and calculations used in sizing equipment, and also indicating how equipment will operate as a system to meet the performance requirements of the access control and alarm monitoring system.
   3. A description of the operating system and application software.

D. Contract Close-out Submittals:
   1. Operating instructions.
   2. Recommended maintenance required and maintenance intervals.
   3. Parts list, including: wiring and connection diagrams.
   4. Record Documents: Maintained on a separate hard copy set of drawings, elementary diagrams, and wiring diagrams of the access control and alarm monitoring system, accurately reflecting all changes and additions to the access control and alarm monitoring system.

1.5 DELIVERY, STORAGE, AND HANDLING

A. Comply with requirements of Section 01 60 00.
   1. Deliver materials in manufacturer's original, unopened, undamaged containers with identification labels intact.
   2. Store materials protected from exposure to harmful environmental conditions and at temperature conditions recommended by manufacturer.
   3. Handle products and systems in accordance with manufacturer's instructions.

1.6 WARRANTY

A. Project Warranty: Comply with requirements of Section 01 78 36.

B. Manufacturer's Warranty: Submit manufacturer's standard warranty document executed by authorized company official. Manufacturer's warranty is in addition to, and not a limitation of, other rights Owner may have under the Contract Documents.
   1. Warranty Period: Two years from date of Substantial Completion.

2 PRODUCTS

2.1 ACCEPTABLE MANUFACTURER

A. DSX Access Systems, Inc.
10731 Rockwall Road
Dallas, Texas 75238
(214) 553-6140 voice
(214) 553-6147 facsimile
(800) 346-5288 voice

2.2 SERVER or WORKSTATION CONFIGURATION

****

File server is where the database files reside. Comm. server is the PC that has the field controllers connected to it. On a small system one PC may be both the File server and Comm. server. A dedicated file sever is required when 5 workstations are to be utilized thereby requiring a minimum of 6 PCs. A dedicated Comm. server will be required for systems that have multiple modems and multiple direct connect Locations attached to the Comm. server.

****

1. 100% IBM compatible PC approved by Microsoft Corporation for running the Microsoft Windows Windows XP Pro, Vista Business, Windows 7 Pro, or Windows 8 Pro - PC with a 2.8 GHz Pentium processor / 2GB RAM (minimum) or greater depending on system scope. Server 2003, and 2008/R2 will work but not required.

B. Processors:
   a) Pentium 2.8 GHz / 2GB RAM (minimum) Host PC single PC, single Location system, or LAN Workstation for single Location system.
   b) Pentium 3.3 GHz / 2GB RAM (minimum) for LAN Comm. Server or File Server for single Location.
   c) Pentium 3.3 GHz / 4GB RAM (minimum) for LAN Comm. Server and/or combination File Server for multiple Location system.

2. Operating System: XP Pro Svc Pack 2, Windows Vista Business Svc Pack 1, Windows 7 Pro 32/64 bit, Windows 8 Pro 32/64 bit. Server platforms include Server 2000, 2003, 2008, and 2008 R2.
3. Hard Disk: 1 Gigabyte free space.
4. Drives:
   a) 16x CD-ROM drive or higher.
5. Sound Card: Windows compatible; required for sound operations; not required for system operation.
6. Super VGA monitor, 800 x 600 pixels minimum resolution; 17-inch or larger recommended.
7. Backup Device: Windows Compatible backup gear.
8. Peripherals:
   a) Serial Ports: Minimum of 1 for either direct or dial-up modem communications.
   b) Mouse: Microsoft IntelliMouse or equivalent recommended but not required.
   c) Modem: DSX provided external dial-up modem only.
9. LAN:
   a) Adapter Card: Required for LAN applications only. 100Mbit is optimum.
   b) If no LAN is required, an MS Loopback Adapter shall be used.

C. Printer: All Windows XP Pro / Vista Business / Windows 7 /Windows 8 - supported printers; required for transaction hard copy. Not required for system operation.

2.3 SOFTWARE

A. Software: WinDSX or WinDSX-SQL Software, complete with the following features and functions:

1. Access control and alarm monitoring system that conforms to the programming and interface guidelines defined by Microsoft Corporation for XP Pro Svc Pack 2, Windows Vista Business Svc Pack 1, Windows 7 Pro 32/64 bit, Windows 8 Pro

32/64 bit, Windows 2003/2008/2008 R2 Server or Microsoft SQL Server 2005/2008/2008 R2 or 2012 compatible software.

2. Basic Functions:
   a) Access Control.
   b) Activity Monitoring.
   c) Database Management.
   d) Database Reporting.
   e) Point status and overrides.

3. System Capacities:
   a) Support a minimum of 32,000 Locations having grouping capabilities to share cardholder databases between sites.
   b) Support a minimum of 4,096,000 readers or 128 reader-controlled doors per Location.
   c) Support a minimum of 170 different card reader formats
   d) Support 1.6-billion cardholders total or up to 50,000 access codes/cards per Location.
   e) Support a minimum of 32,000 supervised alarm inputs or a minimum of 2048 per Location.
   f) Support a minimum of 32,000 programmable outputs or a minimum of 2048 per Location.
   g) Support up to 32,000 facility codes (site codes) total or a minimum of 2048 per Location.
   h) Support a minimum of 32,000 time zones or a minimum of 2048 per Location with each time zone having 3 holiday overrides
   i) Support a minimum of 32,000 companies/card holder groups.
   j) Support a minimum of 32,000 self-purging/auto-renewing holidays.
   k) Support a minimum of 99 user defined fields per Location.
   l) Support a minimum of 32,000 system operators.
   m) Support a minimum of 32,000 password profiles to determine accessibility of system functions for each operator.
   n) Support a minimum of 999 operator comments.
   o) Support a minimum of 32,000 graphic alarm maps for full input, output, CCTV control, DVR control, and alarm handling.
   p) Support a minimum import of 21 graphic file types for maps.
   q) Support a minimum of 32,000 custom action messages per Location to instruct operator on action required when alarm is received.
   r) Support a minimum of 32,000 ASCII output messages per Location for use to interface with CCTV and pager systems.
   s) Support a minimum of 32,000 input to output links.
   t) Support a minimum of 32,000 code to output links.
   u) Support a minimum of 999 guard tours.
   v) Each controlled entry/exit shall have the ability to be locked (secured) and unlocked (open) up to 4 times a day through time zone programming.
   w) Each monitored input shall have the ability to be armed and disarmed up to 4 times a day through time zone programming.
   x) Each reader/keypad shall have the ability to be enabled/disabled up to 2 times a day through time zone programming.

y) Each card/code shall have the ability to be enabled/disabled up to 4 times per day per entry point through access level programming.

z) Provide for support up to 9999 cameras displayed per workstation with live video and Pan, Tilt, Zoom, Scan and Auxiliary controls in video window.

aa) Support a minimum of 32,000 Access Levels.

bb) Support a minimum of 4 Anti-Passback zones per Location.

4. Basic System Features: These features are considered to be standard without the need for any add-on software or hardware.

a) Shall have up to 1000 Workstations with one site license.

b) Shall have the ability for the main Communications engine portion of the software, or CS.EXE, to run as a service, eliminating the need for an OS logon.

c) Shall have built in prevention for multiple comm servers running at the same time when the software is setup incorrectly.

d) Each workstation shall have access to all features if password profile allows. In addition if workstation is used for other tasks (applications) system has option of having an Alarm Pop-up window appear to alert of pending alarms while the operator is using some other program.

e) Password profiles shall be individually customized to allow or disallow operator access to any program function for each Location.

f) Workstation Event Filtering: Shall allow user to define events and alarms that will be displayed at each workstation. Each workstation shall be able to define and assign time zone controlled filters. In addition if an alarm is unacknowledged (not handled by another workstation) for a preset amount of time the alarm will automatically appear on the filtered workstation.

g) Shall have the ability to sort the location tree by name in Workstation

h) Stackable Device Types: Shall allow for a different Wiegand Device Type to be assigned to each Device and all Devices within the same Location sharing the various formats between them.

i) Threat Level Management: With a click of a mouse, press of a button, or presentation of a Card, the system shall be instantly reconfigured to coincide with the Homeland Security Advisory System and meet any heightened security requirements.

j) CCTV Alarm Interface: Shall allow commands to be sent to CCTV systems during alarms (or input change of state) thru serial ports.

k) Animated Response Graphics: Provide for highlighting Alarms with flashing Icons on graphic maps. The current status of alarm inputs and outputs shall be displayed and constantly updated to display changes in real time through animated Icons.

l) Provide the ability to view and control cameras from the graphic maps.

m) Multimedia Alarm Annunciation: Provide for WAV files to be associated with alarm events for audio annunciation or instructions.

n) Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, and/or option of requiring the operator to enter a comment about disposition of alarm.

o) Provide 99 User Defined Fields for cardholder data. System shall have the ability to run searches and reports off of any combination of these fields. Each UDF can be configured with any combination of the following features. MASK: Determines a specific format that data must comply with. REQUIRED: Operator is required to enter data into field before saving. UNIQUE: Data entered must be unique. DE-ACTIVATE DATE: Data

entered will be evaluated as an additional de-activate date for all cards assigned to this cardholder. NAME ID: Data entered will be considered a unique id for the cardholder. AUTO INCREMENTING CARD NUMBER: Badge serial number that prompts the operator to increment the number each time the badge is printed. UDF DATA IS HIDDEN: The system shall also provide the ability to restrict the viewing of certain UDFs containing sensitive information on a field-by-field basis. SELECT DATA FROM LIST: This allows data to be predefined and lets the user pick one of the selections from a drop down list. The choices and the order in which they are viewed can be predefined. EMAIL ADDRESS: Select this if the entries in this field are Email Addresses. There must be an Email Address - User Defined Field for the implementation of Email Groups and Email Alarm Notification. Any Card Holder to be in an Email Group to receive alarm notifications must have their Email Address defined in this UDF. This must be the full and proper Email Address (no aliases allowed).

p) Time and Attendance reporting shall be provided to match in/out reads and display cumulative time in for each day and cumulative time in for length of the report.

q) Guard Tour: Shall provide ability to Plan, Track and Route tours. Shall produce alarm during tour if guard fails to make a station. Tours can be programmed for sequential or random tour station order.

r) Pager System Interface: Alarms shall be able to activate a pager system with customized message for each input alarm.

s) Floor Select Elevator Control and Reporting: Provide for any Card read to activate any floor from the appropriate Cab and report what floor was selected by which cardholder.

t) After Hours HVAC control: Provide for any Card read to activate or control individual HVAC zones based on access and linking level.

u) A means for importing of custom Icons for representation of Inputs, Outputs, or Cameras shall be provided.

****

This note is for clarification purposes. Standard software allows for the Importing of files for images. Examples would be those images taken with a digital camera and then loaded into the system. Standard system also allows Cropping of Image, Badge building application and full print capabilities. All workstations have full access to images, badge editing and display capability. If live video imaging brought thru a video capture card is desired then a software "key" in the form of "dongle" attached to the PC will be required. This is an optional and additional item.

****

v) Photo ID Badging: Provide ability to import images from bitmap file formats, digital cameras, TWAIN cameras, scanners, or live video. Allows image cropping and editing, WYSIWYG badge building application, and full badge printing/print preview capabilities.

w) Photo Recall on Card Use: Provide means that Images can be automatically displayed on a workstation in response to any card read on any reader, as dictated by Time zone per card reader.

x) Photo Recall on Event Selection: Provide means that Images can be manually displayed on a workstation by clicking on the Access Granted or Denied event.

y) Four Zones of Global Anti-Passback: Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at controller level). In addition each anti-Passback reader can be further designated as Hard, Soft or Timed in each of the four anti-Passback zones.

z) Global IO Linking: Provide that any Input or Output can link to any other Input or Output within the same Location without requiring interaction with the host PC (done at controller level).

aa) Global Code to IO linking: Provide that any access granted event can link to any input or output within the same Location without requiring interaction with the Host PC (done at controller level).

bb) Alarm Automation Interface (Smart Port): Provide High level interface to central station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in the same manner as burglar alarms, using an RS-232 ASCII interface.

cc) Emailing of Alarms: Provide the ability to send alarm notifications by way of Email Groups which shall consist of a single or group of recipients. Within each Email Group, Time Zones shall be available to determine when each group member will receive the alarm notification.

dd) Alarm Echo Offsite Monitoring: Provide the ability to allow a Same software remote access control system at a central site to provide after hours monitoring of other Same software primary access control system(s) via dial-up modems.

ee) Remote Control/Diagnostics: Provide the ability to allow a Same software remote access control system at a central site operator to call the Host PC at a another Same software primary access control system and control inputs, outputs and card readers via dial-up modems without performing a download or affecting the downloaded data.

ff) Visitor Management: Provide for and allow an operator to be restricted to only working with visitors. Shall have ability to enroll codes for visitors and can only assign access levels that have designated as approved for visitors. Provides for an automated Logbook of, visitor name, date and whom visitor contacted.

gg) Shall support the use of Virtual Outputs that do not physically exist but can be programmed in the same manner as any Relay Output in the system.

hh) Shall support a First Man In Rule to prevent doors that normally unlock on a schedule from unlocking when weather or other conditions prevent anyone from traveling to or occupying the location or building.

ii) Shall support a Manager First Rule to be used to keep other employees cards from gaining access to the building when the manager is not on site.

jj) Shall support a Two Man Rule requiring that two different cardholders must use their card before they can gain access to a door.

kk) Shall provide for Hazmat Lockdown situations to quickly lockdown a system during Hazmat alerts, without the need of programming or lengthy downloads.

ll) Shall support Time Zone Control to quickly disable one Time Zone and/or enable another through Time Zone Linking, for applications that call for multiple schedules to control cards or door locks with the ability to switch from one schedule to another without any programming or Time Zone reassignment.

mm) Reports: Provide for but not be limited to:

1) Custom History Report Generation: Reports shall be tailored to exact requirements of who, what, when, where, and report parameters can be stored for future recreation of report.
2) Custom History Reports can be previewed, printed to local or network printer or saved to file.
3) Automatic History Report Generator: Provides history reports to be named, saved, and scheduled for automatic generation, printing and/or emailed.
4) Card Holder Reports shall have options to include complete cardholder data or selected parts as well as ability to be sorted by Name, Card number, Imprinted number or by User Defined Fields.

5) Card Holder By Reader Reports: Provide ability to run Card Holder reports based on who has access to a specific reader or group of readers by selecting the readers from a list.
6) Card Holder By Access Level Reports: Provide ability to run Card Holder reports that display everyone that has been assigned to the specified access level.
7) Card Holder by Output Linking Level Reports: Provide ability to run Card Holder reports that display everyone that has been assigned to the specified Output linking level.
8) Card Holder Photo Roster Report: Provide the ability to print from 1 to 50 card holder pictures per page along with any other card holder data as required.
9) Emergency "Who is IN" report (or Muster report): Provide for one Click operation on tool bar to launch report. "Who is IN" must also have ability to be initiated by alarm defined separately by workstation. Input alarm can be any input on any controller.
10) Support for sites that do not have a PC running workstation to print the report from a remote workstation.
11) Management reports to include but not be limited to, Number Of People With Activity, Card Holders Currently On Site, Ins And Outs, Activity Summary sorted by Company, Daily Activity and Card Holders Currently Not On Site.
12) Number of Uses: Provides total number of uses at specified reader. This report is useful for the billing of after hours HVAC use. Report must have option to be sorted by Cardholder or by Company.
13) Panel Labels report. Provide ability to print out the control panel field documentation including the actual Location of equipment, programming parameters, and wiring identification. The system shall be capable of maintaining system installation data within the system database so that it is available on site at all times.
14) Scheduled Override Report: Allows for a report of Scheduled Overrides programmed in the Workstation screen.
15) Activity/Alarm On Line Printing: Provide activity printers to be used at any workstation, printing all events or just alarms.
16) Device Summary report that will show board type, firmware, and RAM for each device.

nn) Key Control Software: Provide ability to store what (conventional metal) keys are issued and to whom, along with key construction information. Reports can be generated to list everyone that has possession of a specified key. Key assignments can be included in Card Holder Reports.

oo) All messages from PC to controllers and controllers to controllers shall be on a polled network that utilizes check summing and acknowledgement of each message. All communication shall be verified and will automatically be buffered and retransmitted if the message is not acknowledged.

pp) TCP/IP Host PC to Controller Communications: Host PC provides for communications to be redirected through a LAN/WAN to a TCP/IP address, rather than through a conventional serial port connection.

qq) Regional Time Zone Settings: Provide for the adjustment of Time Zone references for both Workstation PC's and sets of controllers based on their physical locale.

rr) Selectable Poll Frequency and Message Time Out settings: Provide means to deal with bandwidth and latency issues for TCP/IP, RF and other PC to Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.

ss) Scheduled Override of individual Input and Outputs. Provide the ability to schedule temporary future date overrides to Arm or Bypass inputs, and

Secure or Open Outputs. A scheduled override shall consist of a start time/date and an action to perform coupled with a stop time/date and action to perform.

tt) Override Groups: Provide Groups (or sets) of inputs and outputs that can be monitored and controlled through one Icon. A summary Icon shall be used to display status of all items in the override group. Override group Icons may be placed on graphic maps and may have Scheduled Overrides applied.

uu) Automatic and Encrypted Backups: Provide for database and history back-ups to be automatically stored (anywhere on network) and encrypted with a 9 character alpha-numeric password which must be used to restore or read data contained in the back-up. Shall provide ability to set the number of automatic sequential back-ups before the oldest backup becomes overwritten, (FIFO mode).

vv) Operator Audit Trail: Provide for recording and reporting of all changes made to the database. This option shall have the ability to be toggled off.

ww) Copy command in database: Provide for like data to copied and then edited for specific requirements, (eliminates redundant data entry).

xx) Inputs, outputs, and maps shall have a display order assigned that determine the order shown under status and over-ride windows.

yy) Cardholder: Provide for but not limited to the following;

1) Shall have the ability to create multi-Location access levels combined with the ability to assign an unlimited number of access levels to a card. Each access level may include any combination of doors from any Location. Each door within the access level may have 4 time zones associated with it.
2) Temporary Access Levels: Provide temporary access levels to be assigned to a card using user defined start and stop dates.
3) Shall have the ability to assign an unlimited number of Access Levels per cardholder.
4) Card Use it or Lose it: Shall be able to specify on a per company basis the length of time a card holder can go without using their card before their card is deactivated.
5) Shall have Name search engine with capabilities such as, can search by Last name, First name, Company, User defined data, Codes not used in “X” days, Skills or by 7 other methods. Shall have ability In Workstation to display anti-Passback status to quickly verify if user is in facility.
6) Multiple De-Activate Dates for Cards: Provide user defined fields to be configured as additional Stop Dates to deactivate any cards assigned to the card holder.
7) Shall have the ability to set a Start/Stop time as well as date for card activation/de-activation.
8) Data Base program shall have Active/De-activate buttons in the tool bar that can quickly change users status. Simultaneous multiple selections is an option.
9) Batch card printing shall be provided as standard.
10) Default Card data can be programmed to speed data entry for sites where most card data will is similar. What is this?
11) Enhanced ASCII File Import Utility shall be provided to allow the importing of cardholder data and images.
12) Provide a Cards Expire When Used At This Reader option that allows readers to be configured to deactivate cards when a card is used at that device. Typically used at Visitor badge return.

zz) Shall Automatically define an Output (reader controlled output relay) and Input (door position switch) with the name of the card reader each time a card reader is added to the system to speed data entry.

aaa) Re-Occurring Holiday Schedules: Provide option for holidays to be set to re-occur each year, preventing holiday from being purged from system once the date passes.

bbb) The date time shall be displayed and printed in the format that matches that of the host PC, referred to as windows short date format.

5. Optional Enhancements: These enhancements are considered to be optional with the need for additional software and/or hardware.

a) A PC Master program that allows a PC to perform the polling and communication duties normally handled by a Location's Master panel. Advantages to this configuration are as follows:

1) Communications to the Slave panels can be routed through multiple serial ports and/or TCP/IP LAN/WAN network connections.
2) Greater control can be exerted over the Master to Slave polling frequency. This allows the system to function over slower communication methods.
3) The communications to the Slave panels can be separated into several different channels that operate simultaneously thus providing a substantial increase in the rate of data collection and data distribution.

b) A Soft I/O program that provides the ability to integrate other external systems such as HVAC, intercom, fire and elevator control via serial data links between the systems.

c) A Hot Swap Redundancy program that provides continued availability of system communications and control through the implementation of Primary and Backup Communications Server PCs.

d) A DVR Driver interface that provides the ability to integrate with various OEM Digital Video Recorders thus allowing stored and live video from the DVR to be accessed from within the Access Control program via a LAN/WAN connection.

2.4 HARDWARE

****

Select 1 starter kit per site, provides site license, to be used on up to 1000 workstations.

****

A. Starter/Update Kit: WinStart:

1. Consists of one copy of the WinDSX software on CD, one copy of the Tech Binder that contains a minimum of 1each of the Software Installation manual, Hardware Installation manual, Design Guide (or Product Catalog), and two separately bound copies of the User's Manual. Provide in version [Current Production release (default)] [or specific Previous to Current release].

WinStart SQL:

2. Consists of one copy of the WinDSX SQL software on CD, one copy of the Tech Binder that contains a minimum of 1each of the Software Installation manual, Hardware Installation manual, Design Guide (or Product Catalog), and two separately bound copies of the User's Manual. Provide in version [Current Production release (default)] [or specific Previous to Current release].

****

Select controller type(s) based on project requirement. Listed below in following order 1048PKG – 8 reader unit, 1042PKG 2 reader unit with possible growth to 8 readers, 1022 stand alone 2 reader unit. Refer to manufacturer's technical literature for specific features of each product.

****

B. Intelligent Controller:

1. Model DSX-1048PKG Intelligent 8 Door I/O Controller:
   a) Designed for eight-door reader/keypad application.
   b) Inputs: 32 EOL supervised inputs
      1) Each capable of 2, 3, or 4 state point monitoring with trouble reports.
   c) Outputs: 8 relay, 8-Open collector outputs, 8 pre-warn, 24 LED drivers as follows:
      1) 8 - Form C, 5 amp rated relay outputs.
      2) 8 - Open collector outputs 100ma
      3) 8 - pre-warn outputs for door being held open sounders.
      4) 24 - LED output Drivers to show lock status and or valid card read status at the reader or keypad.
   d) Basic Features:
      1) UL 294 and UL 1076 compliant.
      2) Complete distributed processing: No reliance on host PC for any decision-making.
      3) Access verifications for all cards performed at controller.
      4) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally at controller AND/OR controller to controller within same Location.
      5) Status LED for each Input
      6) Status LED for each Output
      7) Controller Polled LED.
      8) Separate communication receive and transmit LEDs.
      9) Processor functioning properly LED.
      10) Dynamic Battery load test: Programmable using a spare open collector output to trip the Battery Test Input. Battery test may also be manually initiated thru PC at any time.
      11) Battery Load shed circuit: Once the system is running on battery power the batteries must be disconnected at approximately 9VDC. The batteries must stay disconnected until AC power is restored.
      12) Controller must report to PC; loss of power, and low battery as separate alarms.
      13) Status LED for DC power to Controller.
      14) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
      15) Dynamic memory allocation.
      16) Change to/from auto buffering of all transactions based on communications status.
      17) Point to point RS-485 4 wire controller communications allowing up to 4,000 feet between each 1048PKG.
      18) Wiring Management System that includes wire chases, cable ties and mounting clips.
      19) Silkscreen detailing displays wiring termination and function of all terminals on controller.
      20) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.
   e) Power Supplies: DSX-1040PDP (power distribution panel) and DSX-1040CDM (communications distribution module), Included in 1048PKG
      1) 10-15 VDC, 12 VDC nominal / 10A power for controllers. (Battery backed up).

2) 8-12 VDC 10A / 24 VDC 5.6A power for locks (optional battery backup).
3) 5 VDC .375 amp for 5 volt devices.
4) UL 294 and UL 1076 compliant.
5) AC loss and low battery supervisory outputs.
6) Battery load test control input.
7) Lock power override input.
8) Provides individual fused outputs for 8 locks.
9) Provides for 8 individual sets of termination of Lock wiring and control relay wiring. On removable terminals.

f) Controller Architecture:
1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

g) Compatibility:
1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200 baud 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

h) Memory:
1) RAM: 512K
2) ROM: 512K Flash

i) Communications:
1) Via direct serial port, dial-up modem, or TCP/IP. TCP/IP communications require additional hardware.
2) Communication Ports: PC to controller 1 - RS-232 in; 50 feet max. 50 feet – 4,000 feet requires two MCI modules.
3) Controller to controller in the same enclosure; RS232 via the 1040CDM. 1048 to 1048 regenerative RS485 4,000 feet max via the 1040CDM to other enclosures.
4) 1040CDM (communications distribution module) handles RS232 between controllers in the same enclosure, and serves as RS485 connection point for other 1040 Series PKG units or 1022 controllers in controller network.

j) Physical Specifications:
1) Cabinet: DSX-1040E 15.5 inches wide x 22.5 inches tall x 6 inches deep, key locale. Total Weight: 25.0 lbs.
2) Cabinet: DSX-1040PE 15.5 inches wide x 14 inches tall x 6 Inches deep, key locale. Total Weight: 25.0 lbs.
3) Cabinet Finish: Black powder coat with white silkscreen.
4) Operating Temperature: 32 to 131 degrees F.
5) Operating Humidity: 0-95% RD
6) Battery Charging Output:
Trickle Charge: 13.5 VDC. 500ma, fused.
Standby Time: 11 hours under minimum load and 3.25 hours under maximum load w/ 2-12VDC 7AH battery.

****
1042 PKG Controller is a 2-reader unit with power supply and communication for a possible growth to 8 readers. The 1042PKG may have any 3 of the following controllers added to it. 1042 (2 reader increments), 1043 (16 relay increments), or 1044 (32 input increments).
****

2. Model DSX-1042PKG Intelligent 2 Door I/O Controller:
a) Designed for two-door reader/key pad with future growth capabilities to 8 readers application. May add individual 1042, 1043 or 1044 controllers for additional capacity of Readers, Relays or Inputs.
b) Inputs: 8 EOL supervised inputs
1) Each capable of 2, 3, or 4 state point monitoring with trouble reports.

c) Outputs: 2 relay, 2-Open collector outputs, 2 pre-warn, 6 LED drivers, as follows:
   1) 2 - Form C, 5 amp rated relay outputs.
   2) 2 - Open collector outputs 100ma
   3) 2 - pre-warn outputs for door being held open sounders.
   4) 6 - LED output Drivers to show lock status and or valid card read status at the reader or keypad.

d) Basic Features:
   1) UL 294 and UL 1076 compliant.
   2) Complete distributed processing: Never any reliance on host PC for any decision making.
   3) Access verifications for all cards performed at controller.
   4) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally at controller AND/OR controller to controller within same Location.
   5) Status LED for each Input.
   6) Status LED for each Output.
   7) Controller Polled LED.
   8) Separate communication received and transmitted LEDs.
   9) Processor functioning properly LED.
   10) Dynamic Battery load test: Programmable using a spare output to trip the Battery Test Input. Battery test may also be manually initiated thru PC at any time.
   11) Battery Load shed circuit.
   12) Controller can report to PC a loss of DC power, and low battery as separate alarms.
   13) Status LED for DC power to Controller.
   14) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
   15) Dynamic memory allocation.
   16) Change to/from auto buffering of all transactions based on communications status.
   17) Point to point RS-485 4 wire controller communications allowing up to 4,000 feet between each 1042PKG.
   18) Wiring Management System that includes wire chases, cable ties and mounting clips.
   19) Silkscreen detailing displays wiring termination and function of all terminals on controller.
   20) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.

e) Power Supplies: DSX-1040PDP (power distribution panel) and DSX-1040CDM (communications distribution module), Included in 1042PKG
   1) 10-15 VDC, 12 VDC nominal / 10A power for controllers. (Battery backed up).
   2) 8-12 VDC 10A / 24 VDC 5.6A power for locks (optional battery backup).
   3) 5 VDC @ .375 amps for 5 volt devices.
   4) UL 294 and UL 1076 compliant.
   5) AC loss and low battery supervisory outputs.
   6) Battery load test control input.
   7) Lock power override input.
   8) Provides individual fused output for 8 locks.
   9) Provides for 8 individual sets of termination of Lock wiring and control relay wiring with removable terminals.

f) Controller Architecture:
   1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

g) Compatibility:
   1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200-baud, 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

h) Memory:
   1) RAM: 512K
   2) ROM: 512K Flash

i) Communications:
   1) Via direct serial port, dial-up modem, or TCP/IP. TCP/IP communications require additional hardware.
   2) Communication Ports: PC to controller 1 - RS-232 in; 50 feet max. 50ft – 4,000 feet requires two MCI modules.
   3) Controller to controller in the same enclosure; RS232 via the 1040CDM. 1042 PKG to 1048 PKG to 1022 regenerative RS485 4,000 feet max via the 1040CDM.
   ~~4)~~ 1040CDM (communications distribution module) handles RS232 between controllers in the same enclosure, and serves as RS485 connection point for other 1040 Series PKG units or 1022 controllers in controller network.

j) Physical Specifications:
   1) Cabinet: DSX-1040E 15.5 inches wide x 22.5 inches tall x 6 inches deep, key locale. Total Weight: 25.0 lbs.
   2) Cabinet: DSX-1040PE 15.5 inches wide x 14 inches tall x 6 Inches deep, key locale. Total Weight: 25.0 lbs.
   3) Cabinet Finish: Black powder coat with white silkscreen.
   4) Operating Temperature: 32 to 131 degrees F.
   5) Operating Humidity: 0-95% RD
   ~~6)~~ Battery Charging Output:
   Trickle Charge: 13.5 VDC. 500ma, fused.
   Standby Time: 11 hours under minimum load and 3.25 hours under maximum load w/ 2-12 VDC 7AH battery.

****
A 1042 must be used in conjunction with a 1042PKG (cannot be used as a stand alone controller).
****

3. Model DSX-1042 Intelligent 2 Door I/O Controller:
   a) Designed for two-door card reader/key pad applications. Adds additional 2-reader capacity to the 1042PKG. 3 (three) additional 1042 controllers may be added to the 1042PKG for a total of 8-reader capacity.
   b) Inputs: 8 EOL supervised inputs
      1) Each capable of 2, 3, or 4 state point monitoring with trouble reports.
   c) Outputs: 2 relay, 2-Open collector outputs, 2 pre-warn, 6 LED drivers, as follows:
      1) 2 - Form C, 5 amp rated relay outputs.
      2) 2 - Open collector outputs 100ma
      3) 2 - pre-warn outputs for door being held open sounders.
      4) 6 - LED output Drivers to show lock status and or valid card read status at the reader or keypad.
   d) Basic Features:
      1) UL 294 and UL 1076 compliant.
      2) Complete distributed processing: Never any reliance on host PC for any decision making.
      3) Access verifications for all cards performed at controller.
      4) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally

at controller AND/OR controller to controller within same Location..

5) Status LED for each Input.
6) Status LED for each Output.
7) Controller Polled LED.
8) Separate communication received and transmitted LEDs.
9) Processor functioning properly LED.
10) Status LED for DC power.
11) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
12) Dynamic memory allocation.
13) Change to/from auto buffering of all transactions based on communications status.
14) Point to point RS-232 - 3 wire controller communications within the 1042PKG.
15) Silkscreen detailing displays wiring termination and function of all terminals on controller.
16) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.

e) Controller Architecture:
1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

f) Compatibility:
1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200 baud 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

g) Memory:
1) RAM: 512K
2) ROM: 512K Flash

h) Communications:
1) Controller to controller in the same enclosure; Parallel RS232 via the 1040CDM. 1042 PKG to 1048 PKG to 1022 regenerative RS485 4000 feet max via the 1040CDM.

i) Physical Specifications:
1) DSX-1042 11 inches wide x 4.5 inches tall x 1.5 inches deep.
2) Total Weight: 1.2 lbs.
3) Operating Temperature: 32 to 131 degrees F.
4) Operating Humidity: 0-95% RD

****

A 1043 must be used in conjunction with a 1042PKG (cannot be used as a stand alone controller).

****

4. Model DSX-1043 Intelligent Output Controller:

a) Designed for systems requiring large number of relays for control type of application.
b) Outputs: 16 relays Form C, 5 amp 24 Volts.
c) Inputs: 2 non-supervised NC inputs.
d) 1 Output Override control input.
e) Basic Features:
1) UL 294 and UL 1076 compliant.
2) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally at controller AND/OR controller to controller within same Location.
3) Status LED for each Output.

4) Status LED for each Input.
5) Controller polled LED.
6) Separate communication received and transmitted LEDs.
7) Processor functioning properly LED.
8) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
9) Dynamic memory allocation.
10) Change to/from auto buffering of all transactions based on communications status.
11) Point to point RS-232 - 3 wire controller communications within the 1042PKG.
12) Silkscreen detailing displays wiring termination and function of all terminals on controller.
13) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.
14) Can be connected to Slave 1042\1022 to become an Output Extender adding an additional 12 Outputs to original controller.

f) Controller Architecture:
1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

g) Compatibility:
1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200 baud 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

h) Memory:
1) RAM: 512K
2) ROM: 512K Flash

i) Communications:
1) Controller to controller in the same enclosure; RS232 via the 1040CDM. 1042 PKG to 1048 PKG to 1022 regenerative RS485 4,000 feet max via the 1040CDM.

j) Physical Specifications:
1) DSX-1043 11 inches wide x 4.5 inches tall x 1.5 inches deep.
2) Total Weight: 1.6 lbs.
3) Operating Temperature: 32 to 131 degrees F.
4) Operating Humidity: 0-95% RD.

****

A 1044 must be used in conjunction with a 1042PKG (cannot be used as a stand alone controller).

****

5. Model DSX-1044 Intelligent Input Controller:
a) Designed for systems that require large number of Inputs to be monitored.
b) Inputs: 32 EOL supervised inputs
1) Each capable of 2, 3, or 4 state point monitoring with trouble reports.
c) Outputs: 4-open collector outputs, sink capacity 100ma ea.
d) Basic Features:
1) UL 294 and UL 1076 compliant.
2) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally at controller AND/OR controller to controller within same Location.
3) Status LED for each Input.
4) Status LED for each Output
5) Controller polled LED.
6) Separate communication received and transmitted LEDs.

7) Processor functioning properly LED.
8) Dynamic Battery load test.
9) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
10) Dynamic memory allocation.
11) Change to/from auto buffering of all transactions based on communications status.
12) Silkscreen detailing displays wiring termination and function of all terminals on controller.
13) Real time clock calendar allowing time zone control with holiday overrides.
14) Dynamic memory allocation.
15) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.

e) Controller Architecture:
1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

f) Compatibility:
1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200 baud 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

g) Memory:
1) RAM: 512K
2) ROM: 512K Flash

h) Communications:
1) Controller to controller in the same enclosure; RS232 via the 1040CDM. 1042 PKG to 1048 PKG to 1022 regenerative RS485 4,000 feet max via the 1040CDM.

i) Physical Specifications:
1) DSX-1044 11 inches wide x 4.5 inches tall x 1.5 inches deep.
2) Total Weight: 1.2 lbs.
3) Operating Temperature: 32 to 131 degrees F.
4) Operating Humidity: 0-95% RD

****
1022 is a self-contained 2 reader, 8 input, and 4 relay output intelligent controller with its own power supply and communication module built in.
****

6. Model DSX-1022 Intelligent 2 Door I/O Controller:
a) Designed for two-door reader/key pad application.
b) Inputs: 8 EOL supervised inputs
1) Each capable of 2, 3, or 4 state point monitoring with trouble reports.
c) Outputs: 4 relay, 2 pre-warn, 6 LED drivers as follows:
1) 4 - Form C, 5 amp rated relay outputs fused at 1A.
2) 2 - pre-warn outputs for door being held open sounders.
3) 6 - LED output Drivers to show lock status and or valid card read status at the reader or keypad.
d) Basic Features:
1) UL 294 and UL 1076 compliant.
2) Complete distributed processing. Never any reliance on host PC for any decision making.
3) Access verifications for all cards performed at controller.
4) Linking: Input to Input, Input to Output, Output to Input, Output to Output, Code to Input and Code to Output Linking. Done locally

at controller AND/OR controller to controller within same Location.

5) Status LED for each Input.
6) Status LED for each Output.
7) Controller Polled LED.
8) Separate communication received and transmitted LEDs.
9) Processor functioning properly LED.
10) Trouble LEDs to show Low Battery, Battery Fuse, Aux Power Fuse, 12 VDC Fuse, 5 VDC Fuse, Low AC, and High AC.
11) Dynamic Battery load test.
12) Battery Load shed circuit to preserve batteries under sustained power loss.
13) Controller can report to PC Loss of AC power and low battery as separate alarms. Status LED for AC power to Controller.
14) Fuse in line of On board relay for relay and lock power supply protection.
15) Real time on board clock/calendar generation that is synchronized with host PC clock/calendar.
16) Dynamic memory allocation.
17) Change to/from auto buffering of all transactions based on communications status.
18) Point to point RS-485 4 wire controller communications allowing up to 4,000 feet between each controller.
19) Wiring Management System that includes wire chases, cable ties and mounting clips.
20) Silkscreen detailing displays wiring termination and function of all terminals on controller.
21) Controller operating system resides in Flash ROM that is upgradeable thru the Host PC. Upgrades in controller operating system shall NOT require PROM changes.

e) Power Supplies:
1) 12 VDC 1amp and 5 VDC 300 milliamp for card readers, motion detectors and low current draw sounders. (Battery backed up).

f) Controller Architecture:
1) RDC 186 20 MHz processor, RAM, ROM, and removable field wiring terminals.

g) Compatibility:
1) Controller is compatible with any identification device that transmits data using Wiegand, clock/data, or RS-232 ASCII at 1200 baud 8N1. This includes but is not limited to proximity, barium ferrite, bar code, magnetic stripe, Wiegand, keypads, and biometric readers.

h) Memory:
1) RAM: 512K.
2) ROM: 512K Flash.

i) Communications:
1) Via direct serial port, dial-up modem, or TCP/IP.
2) Communication Ports: PC to controller 1 - RS-232 or 1 - RS-485 in; controller to controller 1 - RS-485 in and 1 - RS-485 out; 1 output extender port. TCP/IP communications require additional hardware.

j) Physical Specifications:
1) Cabinet: 15.5 inches wide x 13.5 inches tall x 6 inches deep, key locale.
2) Module size: 10.5 inches wide x 7.5 inches tall x 1.5 inches deep.
3) Total Weight: 12.6 lbs.
4) Cabinet Finish: Black powder coat with white silkscreen.
5) Operating Temperature: 32 to 131 degrees F.
6) Operating Humidity: 0-95% RD

7) Battery Charging Output:
Trickle Charge: 13.5 VDC. 500ma, fused.
Standby Time: 11 hours under minimum load and 3.25 hours under maximum load w/ 2-12 VDC 7AH battery.

****

Select communication interface type based on the first controller (Master) type or the distance from the Communication Server PC. Interface is required with DSX-1022 It is NOT required if Master if less than 50 feet from Communication Server PC.

****

C. Master Communication Interface:
1. Model DSX-MCI Single Channel RS-232 to RS-485 Converter:
a) Extends data communications between the PC and Master controller beyond the 50 feet limit of RS-232.
b) Can be used as an RS-232 to RS-485 converter.
c) Contains two communications LEDs to reflect the status of transmit and receive data terminals.
d) Contains voltage regulator to step 12 VDC to 9 VDC for Modem use at dial-up sites.

****

Select additional communication interface type(s) based on project requirement. Not required but may be useful to avoid long wire runs, or to use different communication paths to controllers.

****

D. DSX-LAN Communications Interface with Modem Back-Up
1. Model DSX-LAN / DSX-LAN(M)
a) Contains both an RS-232 and RS-485 communication port for connection to any DSX Controller.
b) Auto-sensing for both 10 and 100 Mbit networks.
c) Auto-duplexing for compatibility with any router.
d) Power requirements of only 12 VDC @ 300ma, available from any DSX Controller.
e) Can be ordered with Dial-up (M)odem backup for redundant communications .
f) Can be programmed through a serial port using KB2CW.

E. Quadraplexor:
1. Model DSX-1035 Quadraplexor Communications Multiplexer:
a) Multi-function, protocol independent communications repeater hub.
b) Accepts one RS-232 or RS-485 signal input and supplies one RS-232 signal output and four RS-485 signal outputs.
c) Complete with built-in power supply and battery charging circuit.
d) Use of device allows branch (star configuration) wiring.

F. Single Channel MUX Repeater:
1. Model DSX-485T two Channel RS-485 Mux/Repeater:
a) Two channel repeater, intended for applications where a DSX controller is being added to an existing system containing non-revised (prior to 1993) 1032 and 1033 controllers.

G. Multiple RS-232 Output Module:
1. Model DSX-232MUX, RS-232 Communications Mux:
a) Provides 6, RS-232 serial outputs from either an RS-232 or RS-485 input.
b) Purpose: Connects up to 6 Slave controllers from remote sites to a common Master in a centralized Location.

H. Redundant Communications Server Serial Port Switcher
1. Model DSX-SPS, RS-232 Serial Port Switcher:
a. Consists of one (1) each of the following: DSX-1040E rail mount enclosure, DSX-1040 PDP, DSX-SPST serial port switch trigger module and a DSX-2PC two port controller.
b. Each DSX-2PC provides two switched serial ports. The DSX-SPS comes ready for two ports. Add up to 9 more DSX-2PCs for a total of 20 ports.

c. The Backup Comm. Server must have the same number of serial ports as the Primary Comm. Server plus 1 additional serial port for the connection to the DSX-SPST Serial Port Switch Trigger Module.

****

Select FRB8 (Fused relay board) for use in 1048 PKG or 1042PKG. Converts the open collector output of 1042's or 1044's to form C relays. Mounts in the expansion slot of the 1040E. Refer to manufacturer's technical literature for specific features of each product.

****

I. Open collector Output converter:
   1. DSX-FRB8 8 From C relay outputs:
      a) Converts 8 open collector outputs to Form C relays rated at 5 amps.
      b) Fuse in series with each common of each relay to protect relay and lock power supply.
      c) Connects to 1048PKG or 1042PKG.
      d) LED for each relay to show activation.

****

Select reader interface type based on project requirement. Most reader types will NOT require an interface.

****

J. Reader Interface:
   1. Model DSX-CKI-C Cardkey Card Reader Interface:
      a) Allows Cardkey™ Wiegand or Magstripe readers to be connected to system, converts one wire data into two wire data.
      b) One module required for every two readers connected.
   2. Model DSX-CKI-K Cardkey Card Reader plus Keypad Interface:
      a) Allows combination Cardkey™ Wiegand/Keypad readers or Cardkey™ Magstripe Reader/Keypad readers to be connected to system, converts one wire data in to two wire data.
      b) One module required for every two readers connected.
   3. Model DSX-PCI Reader Interface:
      a) Provides interface between existing PCSC™ Barium Ferrite Swipe and Insert readers and controller.
      b) Supports 2 PCSC swipe or insert readers.
      c) One module required for every two readers connected.
   4. Model DSX-CPI Reader Interface:
      a) Provides interface between existing CheckPoint™ proximity readers and controller.
      b) Supports 1 Checkpoint™ reader.
      c) One module required for each reader connected.
   5. Model DSX-WMI Reader Interface:
      a) Provides interface between existing WaterMark readers and controller.
      b) Supports 2 WaterMark readers.
      c) One module required for every two readers connected.
   6. Model DSX-RKM Reader Interface:
      a) Provides interface between existing Radionics ReadyKey™ proximity readers and controller.
      b) Supports 2 readers.
      c) One module required for every two readers connected.
   7. Model DSX-AMI Reader Interface:
      a) Provides interface between existing American Magnetics™ magnetic stripe readers and controller.
      b) Supports 1 reader.
      ~~c)~~ One module required for each reader connected.

****

Time Display Module displays system time at readers. Used for Time and Attendance .

****

K. Time Display Module Model DSX-TDM:
   1. 4 digit LED time display Module.
   2. Housing: Black aluminum.
   3. Display Height: 1 inch to 5 inch

4. Synchronization: Minimum - Once each minute.

****

Noise filter used primarily for card readers located in elevator cabs (recommended for those installations).

****

L. Card Reader Cable Noise Filter Model DSX-220:
1. Designed for use in harsh environments where RF or electrical noise is induced on the cable.
2. Serves as a data line extender for service up to 1500 feet from controller.
3. Two piece device, one each installed at controller and the other at the reader, (requires 12VDC power at controller and 12VAC at reader).

****

Data protection module should be used anytime data communications exits or enters a building. Select type of data protection circuit below 1a)-RS232 OR 1b) RS485

****

M. Data Protection Module:
1. Provided with 3-stage surge protection, one module required at each end of communication line.
a) [Model DSX-DP232, RS232 Date Surge Protection Module].
b) [Model DSX-DP485, RS485 Data Surge Protection Module].

****

Extra enclosures may be used for termination of additional wiring or for controllers that were "special ordered" without enclosures. (Standard controllers come with enclosures). Based on size desired or type of controller select 4a) or 4b)

****

N. Additional Controller Enclosure(s): DSX-1040E.
1. Six Slot Equipment Enclosure with Lock and Key. Accepts 4 1040 Series controllers, one 1040CDM and one expansion slot.
2. Provided complete with wire channels, conduit knockouts, and wire tie anchors.
3. Constructed of 18-gage powder coated steel, black color, with white silk-screened cabinet identifications.
4. Depth: 6 inches deep.
a) Face dimensions: [15.75 inches wide x 22.75 inches high]

****

Video Imaging Hardware should be included if required. Select Image Key and CamKit for assembly in customer provided PC.

****

O. Image Key:
1. Provides a hardware key that is required for live image capture.

P. CamKit:
1. Provides a USB Camera, Lens, built in Flash Unit, Cable, and Tripod, to be configured on customer supplied PC.
2. CamKit requires Image Key for Live Image Capture but is not required.

2.5 SYSTEM OPERATION AND CONTROL SPECIFICATIONS

A. System Integrity and Performance

1. Each controller shall operate as an autonomous intelligent processing unit. It shall be part of a fully distributed processing control network. Each controller shall maintain its own database, in its entirety, necessary for independent operation in its own RAM. It shall make all decisions about access control, alarm monitoring, linking functions and door locking schedules for its operation independent of any other system components.

2. When controller is brought on-line all database parameters shall be automatically downloaded to it. After initial download is completed only database changes shall be downloaded to each controller. This shall be referred to as "Incremental downloads" or "Downloading of Changes Only".

3. I/O Linking and Anti-Passback functions shall operate globally between all controllers within the same Location without any Host PC intervention. Linking and Anti-Passback functions shall not depend on any decision-making process or macros from the Host PC and shall occur even with the Host PC off line.

4. Controller operating system resides in Flash ROM that is upgradeable thru a download from the Host PC. Upgrades in controller operating system shall NOT require PROM changes.
5. A Location shall be defined as a loop of up to 64 controllers (128 devices).
6. The first controller of every Location shall be designated as the “Master”. All subsequent controllers at the same Location shall be designated as “Slaves”. Any controller may be selected by dipswitch settings to work as a Master controller. A Master controller shall perform all the same functions as a Slave controller, but it shall also be responsible for polling all Slave controllers and reporting the history transactions to the host PC. The Master controller shall not make any access decisions for the Slave controllers. The Master controller shall be the messenger for information from the controllers to the PC, and from the PC to the controllers.
7. Each card reader port of a controller shall be custom configurable for over 230 different card reader or keypad formats. Multiple card reader/keypad formats may be used simultaneously at different controllers and even within the same controller.
8. The Controller shall provide a response to all Card Read or Keypad entries in less than .25 seconds regardless of System size.
9. All valid codes for a Location shall be downloaded and reside in the controllers. The controllers shall not depend on querying the Host PC database or any other controller or system component for code authorizations.
10. All communication between the Host PC & Master controller (Direct, Dial-up or TCP/IP), and between the Master & Slave controllers use a polled communication protocol that checksum and acknowledges (ACK) each message. All communication is verified and will automatically be buffered and retransmitted if it fails to be acknowledged.
11. There shall be NO degradation of System performance in the event of a communication loss between the Host PC and the Master controller. The Master controller shall automatically switch to buffer mode storing up to 10,000 events. There shall be NO loss of transactions in System history files until the controller buffer overflows.
12. A missing or failed controller shall not degrade the performance of the communicating controllers in the controller communication network. Missing controllers shall be ignored and sampled less often by the Master controller. Any functioning Slave controller not communicating with the Master will automatically switch to buffer mode storing up to 10,000 events.
13. Buffered events shall be handled in a FIFO (First in First Out) mode of operation.
14. All controllers shall have a built in dead man reset timer (watchdog circuit) that automatically reboots the controller in the event the processor is interrupted for any reason.
15. Any controller that is reset, or powered up form a non-powered state shall automatically request a parameter download and reboot to its proper working state. This shall happen with out any operator intervention.
16. The System shall provide a means for viewing the Communications Status of the intelligent controllers RS485 Communications loop.
17. The Communication Status window shall display which controllers are currently communicating, a total count of missed polls since midnight, and which intelligent controller last missed a poll. Missed polls reflect that messages had to be retransmitted and are an indication to the soundness or quality of the controller-to-controller network.
18. The Communication Status window shall show what type of CPU, what type of Input/Output board, and how much RAM Memory each controller has.
19. The chance that a controller will allow access to an unauthorized individual under normal operating conditions shall be less than 1 in 10,000.

20. The chance that an authorized individual will be denied access under normal operating conditions shall be less than 1 in 1,000.

B. PC to Controller Communications (All Types)

1. The System shall communicate using Serial ports for direct connections, and/or TCP/IP LAN and/or dial-up Modems for connections to Locations.
2. The System shall be able to use either one or both serial ports for dial-up modems, and either one or both serial ports for direct connect Locations and/or TCP/IP LAN connect Locations.
3. The serial ports used for communications shall be individually configurable for Direct Communications, Modem Communications Incoming & Outgoing, or Modem Communications Incoming only, or as an ASCII output port.
4. If more than 2 serial ports are needed, a Windows compatible Multi-Port Communications Board shall be used.
   a) The outboard multi-port serial board shall connect to an internal PCI bus adapter card. The port expander boards shall have an expandable and modular design. The port expansion modules shall be available in a 4, 8, or 16 Serial Port Configuration that is expandable to 32 or 64 serial ports.
   b) The Multi-Port Comm. Board shall allow multiple direct connect Masters to be connected to the System.
   c) The Multi-Port Comm. Board shall allow multiple dial-up modems to be connected to the System.
5. Direct serial, TCP/IP and Dial-up Modem Communications shall have no difference in monitoring or control of the System with the exception of the connection that must first be made to a dial-up Location.
6. For TCP/IP communications an option to set the Poll Frequency and Message Response Time Out settings shall be available. This will allow tuning for bandwidth and latency issues associated with network communications.

C. Direct Serial or TCP/IP PC to Controller Communications

1. The communication software on the PC shall supervise the Controller to PC Communications link.
2. The communications shall be supervised when using either direct serial port connections, or TCP/IP LAN connections.
3. Loss of communications to any Master Controller shall result in a Communication loss alarm at all PCs running the communications software. The Master controller shall then automatically buffer events.
4. When communications is restored to the Master Controller all buffered events shall automatically upload to the PC and any database changes shall automatically be sent to the Master controller.

D. Dial-up Modem PC to Controller Communications

1. The communication software on the PC shall supervise the Controller to PC Communications link during dial-up modem connect times.
2. The System shall be programmable to routinely poll each of the remote dial-up modem Locations collecting event logs and verifying phone lines each at different time intervals.
3. The System shall be programmable to dial and connect to all dial-up modem Locations and retrieve the accrued history transactions on an automatic basis as often as once every 10 minutes to once every 9999 minutes.
4. Failure to Communicate to a dial-up Location 3 times in a row shall result in an alarm at the PC.
5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the Host PC will be set to and maintained at the proper local time. This feature shall allow for geographical time zones that are ahead or behind the host PC.

6. The Master of a dial-up modem-connected Location shall automatically buffer all normal transactions until it's buffer reaches 80% of capacity. When the transaction buffer reaches 80% the Master controller shall automatically initiate a phone call to the central monitoring PC and upload all transactions.

7. If an alarm event occurs, the Master controller shall initiate an immediate call to the PC to report the alarm event.

8. Modem Communications shall allow the use of 9600-baud dial-up modems provided by the manufacture of the System. Modems used at the Master Controller shall be powered and battery backed up by the controller.

E. Controller to Controller Communications

1. The Controller to Controller Communications shall be a true RS-485, 4-wire, point to point, regenerative (repeater) communications network methodology.

2. The RS-485 communications signal shall be re-generated at each controller without any additional modules or hardware.

3. The controller-to-controller communications shall be performed without the use of external modules or devices.

4. The Master Controller shall supervise the communications to each Slave controller. Communication Loss shall be reported immediately for direct serial port connected Locations. Controller communications loss shall be configurable to initiate a call to the PC for dial-up modem Locations.

F. Database Downloads

1. Controllers shall initially be downloaded with all Location data.

2. The System shall download all database changes to the intelligent controllers utilizing automatic non-invasive incremental updates also known as the Downloading of Changes Only.

3. When data is downloaded from the PC to the Master controller the PC shall request a complete database checksum to check the integrity of the download. If the data checksum does not match the PC, the full data download shall automatically be retransmitted to the Master controller.

4. When data is downloaded from the Master controller to a Slave controller the Master controller shall request a complete database checksum to check the integrity of the download. If the data checksum does not match the Master, the full data download shall automatically be retransmitted to the Slave controller.

5. When data is transferred from the Master controller to the Slave controllers the integrity of the data download is verified through checksums. A check sum on each message, each table, and a final table total checksum are calculated. If the checksums do not match the Masters the data shall be automatically retransmitted from the Master to Slave.

6. If the Master controller is reset for any reason, it shall automatically request a database parameter download from the PC. When the Master is a dial-up modem connect Location, it shall automatically dial the PC, and request and receive the database parameter download. The download shall restore the remote site to its normal working state and shall take place with no operator intervention.

7. Slave controllers that have lost communication with the Master controller upon restoral shall have their database evaluated by the Master Controller. If the controllers' database is still current the controller is brought back on-line without downloading. If the controllers' database is not current it is brought back on-line and then fully downloaded. This download shall restore the Slave controller to its normal working state and shall take place with no operator intervention.

8. When changes are made to the database for a dial-up modem Location the PC shall automatically call and download those changes to that Location. No operator commands shall be necessary.

9. The System shall have the ability to schedule the download of changed data to a dial-up Location (for lower phone rates) between the hours of 2 and 5 AM.

10. The System shall also allow the data changes to be downloaded immediately or after a programmable delay from 1-999 minutes (prevents system from multiple sequential phone calls when editing a dial-up Locations' data).

G. Alarm Response and Handling

1. The System shall have manual and automatic responses to incoming point status change or alarms.

2. Each input shall have the ability to respond automatically with a link to inputs and or outputs, operator response plans, unique sound with the use of WAV files, maps or images that graphically represent the point Location.

3. Maps shall automatically display for each input assigned to it that has gone into alarm if the option is selected on a per input basis.

4. Alarm handling shall require a two-step process. When the alarm is first responded to it will be referred to as Acknowledged. This shall silence alarm beeping and any alarm WAV files being played. The alarm is then referred to as acknowledged but Un-Resolved. The next handling of the alarm will give the operator the ability to give a resolution (or operator comment) as to the final deposition of the event. The alarm shall then clear.

5. Each workstation shall display the total pending alarms and total un-resolved alarms.

6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.

7. Alarms shall be reported in a real time fashion barring any connection time for non-direct connect (dial-up) Locations to the Host PC where the operator shall be alerted and given an optional response plan or Action Message.

8. Operator response action messages shall be a minimum of 65,000 characters each with up to 32,000 messages.

9. Alarms shall be displayed and can be handled from a minimum of 4 different windows.
   a) The input status window: The status Icon will be overlaid with a large red blinking Icon. Selecting the Icon will acknowledge the alarm.
   b) The History log transaction window: The name, time, and date will display in red text. Selecting the red text will acknowledge the alarm.
   c) The Alarm log transaction window: The name, time, and date will display in red verbose. Selecting the red text will acknowledge the alarm.
   d) The graphic map display: The Icon for the input in alarm will flash with a large red blinking Icon. Selecting the Icon will acknowledge the alarm

10. Once the operator has acknowledged the alarm, they shall be automatically prompted to enter comments as to the nature of, and action taken on the alarm. The operator comments may be manually entered or selected from a predefined list or a combination of both.

11. Predefined Operator Comments shall have the ability to be used to resolve alarms where there are regular alarm occurrences. The operator shall have the means to choose from a list instead of typing the same message repeatedly.

12. The System shall track when and who acknowledged and resolved the alarm.

13. All identical alarms (from the same alarm point) shall be acknowledged at the same time the operator acknowledges the first one. All identical alarms shall be resolved when the first alarm is resolved. Restoral conditions, if set to be acknowledged shall follow the same operation as just described above for alarms.

14. The user shall have the ability to manually command inputs to arm, bypass, or follow their Time Zone from the PC with a one step command.

15. The System shall have an alarm popup message window and beep that informs the operator of an alarm that is pending. This shall occur even when the alarm monitoring application is not the top window.
16. The alarm popup message window shall display the alarm and precisely identify the point.
17. The popup alarm window shall also provide the operator the opportunity to ignore the alarm and clear the popup window or to jump to the alarm-handling window and deal with the alarm and any subsequent alarms.
18. Alarm Messages shall be receivable by the PC even when the PC is downloading or retrieving a Log from the Location Master.
19. The System shall have the ability to acknowledge and resolve alarms and control inputs and outputs during a download and Log retrieval.
20. When a reader-controlled output (relay) is opened the corresponding alarm point will automatically be bypassed.
21. All alarm points located on System controllers, with the exception of the 1043, shall accommodate 2,3,and 4-state point monitoring with trouble conditions.
22. All inputs, with the exception of the 1043 shall be individually programmable with at least 5 different circuit types to choose from.

H. Input and Output Control

1. All inputs in the System shall have two Icons representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs the Icons shall respond by changing and updating to the proper Icon to display that input's current state in real time. These Icons shall also display the inputs armed or bypassed state, and whether the input is in the armed or bypassed state due to a time zone or by a manual command.
3. All outputs in the System shall have two Icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. When viewing and controlling outputs the Icons shall respond by changing and updating to the proper Icon for that points current state in real time. These Icons shall also display whether the output is in the secured or open state due to a time zone or by a manual command.
5. Animation: The Icons used to display status of the Input or Output points shall be constantly updated without any prompting by the operator to show their current real time condition.
6. The operator shall be able to scroll the list of Inputs or Outputs and press the appropriate button on toolbar or right click to perform the desired function: arm, bypass or set to time zone for inputs, and secure, open, or set to time zone for outputs.
7. Graphic Maps containing Inputs, Outputs and Override groups:
   a) Full color Maps shall be importable from most any graphics file format. Maps shall allow for all input, output, and override group Icons to be placed on the maps in an easy one step drag and drop method.
   b) Maps shall provide real-time display animation and allow for control of all points assigned to it.
   c) The System shall allow the same inputs, outputs, and override groups to be defined on different maps. There shall also be the ability to navigate from one map to the next that the points are defined on. There shall also reside the ability to order or prioritize the order in which the Maps will be displayed.
8. Override Groups containing Inputs and Outputs:
   a) The System shall incorporate override groups that provide the operator with the status and control over user defined "sets" of inputs and outputs with a single Icon.

b) The Icon shall change automatically to show the live summary status of all points in that group.
c) The Override Group Icon shall provide a method to manually control or set to time zone all points in the group.
d) The Override Group Icon shall allow the expanding of the group to show the Icons representing the live status for each point in the group, individual control over each point and the ability to compress the individual Icons back into one summary Icon.

9. Schedule Overrides of Inputs, Outputs and Override Groups:
a) To accommodate temporary schedule changes that do not fall within the holiday parameters the system shall incorporate scheduled overrides individually for each input, output, and override group in the System.
b) Each schedule shall be comprised of a minimum of two dates with separate times for each date.
c) The first time and date shall be assigned the Override State the point shall advance to, when the time and date become current.
d) The second time and date shall be assigned the state in which the point shall return to, when that time and date becomes current.

I. I/O Linking

1. The System shall support I/O Linking, which is an action initiated by an input, output, or card read that causes a reaction within a group of inputs and/or outputs. Linking to an input controls its armed state. Linking to an output controls its on/off state.
2. In regard to the before mentioned Linking characteristics the System shall fully facilitate Input to Input Linking, Input to Output Linking, Output to Output Linking, Output to Input Linking, Code to Input, and Code to Output Linking.
3. All Input, Output, and Code Linking shall operate on a global level within a Location. Global linking is any input, output, or card read use can initiate a link from any controller in the Location to any inputs and/or outputs on any controller(s) within the same Location without any interaction with the host PC.
4. The System shall provide Linking initiated by an input change of state or an input alarm.
5. The System shall provide Linking initiated by the transition of an output from secure to open and the transition from open to secure.
6. Code to input and/or output linking shall be initiated by a designated code used at a designated reader/keypad.
7. The reader/keypad used will determine which group of inputs and/or outputs will be activated. That is the same card can cause a different link to occur based on which reader the card was read at.
8. Responses to links shall include: follow, latch, pulse, toggle, and return to time zone.
9. In addition to inputs and outputs, time zones shall also have the ability to receive a link from an input, output, or card read. Within each time zone definition, there shall be the option for the time zone to be “On” or “Off” when a link is received.

J. LAN Installations

1. The Local Area Network shall allow multi-user capabilities to the system. It shall allow all functions to be executed at every Workstation on the LAN running the WinDSX software.
2. The software, running on a LAN, shall support as few as 2 Workstations or as many as 1000.
3. The System software shall be Local Area Network (LAN) compatible without any software supplements or upgrades.

4. The system shall be compatible with Windows XP Pro Svc Pack 2, Windows Vista Business Svc Pack 1, Windows 7 Pro 32/64 bit, Windows 8 Pro 32/64 bit.
5. The system shall utilize TCP/IP as the primary protocol.
6. The software shall be installed on the local hard disk of each Workstation so that each Workstation shall run the executable files of the program from the local hard disk, but reference the shared database on the File Server.
7. One PC shall be designated as the Comm. Server. This PC shall have the actual physical connection to the Intelligent Controllers by way of Direct Serial Port Connection, Dial-Up Phone Modem, or TCP/IP.
8. All Workstations shall have full control capabilities over the controllers. They shall be able to perform all administrative duties such as Reports and Database Management, and interact with a local or remote site as operator password privileges allow.

2.6 DATA BASE AND SYSTEM FEATURE SPECIFICATIONS

A. Database Operation

1. The System data management program general layout shall be in a hierarchical menu tree format with simple navigation through expandable menu branches and manipulated with the use of menus and Icons in a main menu and System toolbar.
2. The System shall use standard Icons in the toolbar for Add, Delete, Copy, Print, Capture Image, Activate, Deactivate, and Who-Is-In (Muster) report.
3. The System shall be programmable with English prompts, scrollable menus, and pull down windows.
4. All data entry shall automatically be checked for duplicate and illegal data. This field verification shall be used to insure that proper information is entered into the System.
5. The Database Management Program shall provide a Point and Click approach to data manipulation.
6. Upon making a selection in database, the view window shall immediately display a list of records for the selected topic. From the view window Add, Edit, or Delete commands may be selected. The process of adding, editing or deleting will then return operator to the View Mode giving immediate visual feedback to all the program entries, existing or those just changed.
7. There shall be a memo or note field for each item that is stored in the data. These note fields are useful for storing information about any defining characteristics of the item. These could be but are not limited to; the Location of, what purpose item was entered for, or reasons changes were made.
8. There shall be a next and previous command buttons visible when editing any database field for quickly navigating from one record to the next.
9. There shall be a copy command and copy tool in the tool bar to copy data from one record for the purpose of creating a new similar record.
10. The system shall check all database entries for valid data and shall automatically display an error describing any invalid data.

B. File Management

1. The operator shall be able to backup the System data at any time and may define that backups be performed unattended.
2. The Backup program shall be an integral part of the access control software. The backup System shall be easy to use with menu guidance.
3. The System shall incorporate an Integral Database Backup and Restoration System with selectable target media including any Windows logical drive, Zip drives, and network resources as a minimum.
4. The System Backup feature shall have both a Manual and Automatic mode of operation.
5. The System shall incorporate a Manual and Auto-Backup History feature that allows history to be backed up to a specified target and storage media including Windows compatible logical drives, Zip drives, and network resources as a minimum.

6. The System shall incorporate database restoration features that allow data to be selectively restored.
7. The backup program shall provide manual operation from any PC on the LAN and shall operate while the system remains operational.

C. Operator Passwords
1. The software shall support up to 32,000 individual operators each with a unique password.
2. Each password shall be from 6 to 10 alphanumeric characters.
3. Passwords shall be capable of being case sensitive.
4. The password shall be hidden and never displayed when entered.
5. Each password shall accept a unique and customizable password profile with the ability for several operators to share a password profile.
6. There shall be 32,000 definable operator password profiles.
7. One password profile shall be predetermined for access to all functions and areas of the program.
8. Each password profile may be customized to allow or disallow operator access to any program operation.
9. All software functions shall have the ability to restrict operators through settings in a password profile.
10. All database functions such as View, Add, Edit, and Delete shall have the ability to restrict operators by settings in a password profile.
11. Password restriction shall apply to each input and output individually. This restriction specifies which inputs and outputs the operator is able to manually manipulate.
12. Password shall be able to restrict which doors an operator can assign access to.
13. Operators shall use a User Name and Password to log on the System.
14. The same User Name and Password is used to access all areas and all programs.
15. Once logged on, only those menu items and functions that the operator is authorized for based on the operator's password profile are displayed.
16. There shall be an Icon that allows the operator to log off without fully exiting the program. User may be logged off but the program will remain running. The logon window shall then be displayed for the next operator.
17. The system shall have the ability to hide the user name of the previous operator logged on.
18. Where "Strong or Complex" password utilization is required WinDSX SQL can use Active Directory to authenticate operators. Once allowed in by AD the operator is still controlled by their password profile.

D. Hardware Location Password
1. There shall be a Location password that will be utilized for PC to Dial-up Modem sites to prevent unauthorized communications with the Location.
2. Each Location password shall be from 1 to 8 alphanumeric characters.
   a) The Location Password shall be verified with the dial-up Location Master controller before communication proceeds.

E. Reports and History
1. All history shall be initially stored on the hard disk of the host PC.
2. The system shall have the ability to view the History on any workstation or print History to any system printer.
3. All History Reports shall allow the user to select any date, time, event type, device, output, input, operator, Location, name, or cardholders to be included or excluded from the report.
4. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
5. Each report shall depict the date, time, event type, event description, device, or input/output name, cardholder company assignment, and the cardholder name or code number.
6. Each line of a printed report shall be numbered to insure that the integrity of the report has not been compromised.

7. The total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms" the total shall reflect how many alarms occurred during that period.
8. All reports shall have the 3 following options:
   a) View on Screen.
   b) Print to System Printer.
   c) Save to File with full path statement.
9. The System shall have the ability to produce a report indicating either:
   a) The status of the Systems inputs and outputs.
   b) The inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.
10. The System shall facilitate a Custom Code List Engine which allows the Access Codes of the System to be sorted and printed according to the following criteria:
    a) Active, Inactive, or Future Activate or De-activate
    b) Code number, Name, or Imprinted Card Number
    c) Company, Location, Access Levels
    d) Start and Stop Code Range
    e) Codes that have not been used since X number of days
    f) In, Out, or Either status
    g) Codes with Trace Designation
11. The System shall incorporate a Who Is In (Muster) report; One Button Report for cardholder locating. This report shall contain a count of all persons that are “In”, Location wide, and a count with detailed listing of name, date and time of last use, grouped by the last reader used or by the company assignment. This report shall also be generated from a pre-defined alarm input. Any Workstation in the system shall be able to print the report for a particular Location.
12. The reports of the systems database shall allow options such that every data field may be printed.
13. The reports of the systems database shall be constructed such that the actual position of the printed data shall closely match the position of the data on the data entry windows.

F. Graphics
1. The software shall support 32,000 Graphic Display Maps. . The system shall allow the maps to be imported from a minimum of 21 standard formats from another draw or graphics program including AutoCad™.
2. All Inputs and Outputs shall have the ability to be placed on any graphic map in a drag and drop method.
3. Graphic maps shall display automatically the real time state of outputs and inputs in an animated fashion.
4. Camera Icons shall have the ability to be placed on any graphic map that when selected will open a live video window and display the camera associated with that Icon and provide for real time Pan/Tilt/Zoom control.
5. Any Input, Output or Camera placed on a map shall allow the ability to Arm or Bypass an input, Open or Secure an output, or control the Pan/Tilt/Zoom function of any camera.
6. Any alarm input activation shall optionally by input automatically pull up a graphic map associated with the alarm.
7. Any alarm activation shall give the operator the ability to manually pull up a graphic map associated with the alarm.
8. The operator shall be able to view the inputs or outputs and the point's name by simply moving the mouse cursor over the point on any graphic map.
9. All inputs and outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view all Graphic Maps associated with any input or output.
10. Each graphic map shall have a display order sequence number associated with it to provide a predetermined order when toggled to different views.
11. Map size shall be configurable for each map.

G. Help
1. All main menus shall have a Help option listed.

2. The System Help selection shall provide a unique and descriptive context sensitive Help System for all selections and functions with the press of one function key.
3. The Help System shall provide a manner of navigation to any specific topic from within the first Help window.
4. The help system shall be accessible outside the program.

H. Access Card/Code Operation and Management
1. Access authorization shall support verification of the card/code by facility code (if implemented) first, by card/code and/or Pin validation second, by access level (time of day, day of week, date), by anti-Passback status, and by number of uses.
2. The System shall allow multiple cards/codes to be assigned to a cardholder.
3. Each card/code assigned to a cardholder shall have the ability for an unlimited number of access levels assigned to it across all Locations. Each access level shall have any combination of doors in it. Each door shall have the ability to have 4 time zones associated with it.
4. The System shall allow the grouping of Locations that allows cardholder data to be shared by all Locations in the group, thus preventing the redundant data entry.
5. The System shall facilitate the viewing, building, editing and issuing of access levels from the code entry window, through an Access Level Manager Engine that maintains and coordinates all access levels to prevent duplication or the incorrect building of levels.
6. The System shall allow a person to be entered into the System for visitor, data tracking or photo ID purposes without assigning that person a card or code.
7. Key Tracking shall be an integral function of Cardholder data. This shall allow the tracking and accountability of lock hardware keys (metal keys) issued to each cardholder. Reports can be generated displaying all keys assigned to this cardholder or all cardholders that have a specific key.
8. The System shall provide a special audible and visual annunciation at the PC when a card/code selected to be traced is used at designated trace readers. In addition cardholder image shall be automatically displayed when a traced card is used at designated trace readers.
9. The System shall allow each Card Holder to be given either an unlimited number of uses or a number range from 1-9998 that regulates the number of times the card can be used before it is automatically disabled.
10. The System shall allow cards/codes to be activated and de-activated manually or automatically by date as well as time. The System shall allow for multiple de-activate dates to be pre-programmed.
11. The System shall have the ability to de-activate cards/codes by company based on lack of use for a pre-defined number of days.
12. Integral Photo ID Badging and Photo Verification shall use the same database as the Access Control System and may query data from cardholder, company, and other personal information to build a custom ID badge.
13. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
14. The System shall allow a means of grouping cardholders together by Company (department) or other characteristic for a more efficient method of reporting on and enabling/disabling cards/codes.
15. The Access Codes may be up to 12 digits in length.

I. Facility Codes
1. The System shall accommodate up to 2048 Facility Codes per Location with the option of allowing the Facility Codes to work at all doors or just particular doors.

J. Operator Comments
1. With the press of one appropriate button on the toolbar the user shall be permitted to make Operator Comments into History at anytime.
2. Automatic prompting of Operator comment shall occur before the resolution of each alarm.
3. Operator Comments shall be recorded with time, date, and operator number.
4. Comments shall be sorted and viewed through Reports and History.
5. The operator comments shall comprise of two parts and either or both may be utilized, predefined or manually entered.

a) Manually entered through keyboard data entry (typed) up to 65,000 characters per each alarm
b) Predefined and stored in the database for retrieval upon request.

6. The system shall have a minimum of 999 Predefined Operator Comments with up to 30 characters per comment. The Operator Comments that can be manually entered shall accept up to 65,000 characters per Comment.
7. Predefined Operator Comments shall have the ability to be used to resolve alarms where there are regular alarm occurrences. The operator shall have the means to choose from a list instead of typing the same message repeatedly.

K. Company
1. The System shall provide a means of assigning one of 32,000 company names to a group of cardholders.
2. Company names may be used to separate cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, or division of a company the person belongs.
3. The software shall have the ability to deactivate and re-activate all codes assigned to a particular company with one action.
4. History reports and code list printouts shall have provisions to be sorted by Company name.
5. Company names shall provide a means to give managers reports that pertain to their personnel only.

L. Time Zones
1. The System shall allow up to 32,000 Time Zones for each of the 32,000 Locations.
2. Each Time Zone shall contain a start and stop time for 7 the days of the week and 3 separate holiday schedules.
3. A Time Zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm/disarm, when an output shall automatically open/secure, or when cards assigned to an access level shall be denied or granted access.
4. Dynamically linked bar graphs shall display the resultant active and inactive times for each day and holiday as start and stop times are entered or edited.
5. The System shall allow for up to 4 different Time Zones to be assigned to any input, output.

M. Holidays
1. The System shall have provisions for 32,000 Holidays.
2. Each Holiday shall be defined with MM/DD/YYYY and a description.
3. Up to 32,000 holidays may be entered in advance.
4. Holidays shall be defined as a minimum of three types. This will allow for 3 separate holiday schedules.
5. Holidays shall have an option to be designated as occurrence each year, those shall remain in system and not be purged.
6. Holidays not designated to occur each year shall be automatically purged from the database after the date expires and a new Holiday is added.
7. Each Holiday shall have the ability to be assigned to one of three types of Holiday. The type of holiday shall be relative to a time period of one twenty-four hour period.
8. Holidays may be created per Location or by Location Group.

N. Access Levels
1. The System shall allow for 32,000 access levels.
2. One level shall be predefined as the Master Access Level. The Master Access Level shall work at all doors at all times.
3. The System shall allow for access to be restricted to any area by reader and by time. Access Levels shall determine when and where a card is authorized.
4. The System shall be able to create multiple door and time zone combinations under the same Access Level so that a card may be valid during different time periods at different readers even if the readers are on the same controller.
5. Each door in an access level shall have the ability to have a minimum of 4 different time zones assigned to it.

6. The System shall incorporate an Access Level Manager Engine for menu guidance and assistance in creating, managing, and assigning access levels.
7. The manager shall be accessible from the card data entry window.
8. When assigning an Access Level, the access level manager engine shall provide door and time zone listings for the operator to choose from.
9. The system shall allow for the ability to copy form one door assignment up to 4 time zone schedules with one operation for assignment to another door. This shall reduce operator data entry time when creating access levels that use like time zone schedules.
10. The system shall allow the User to Modify Access Levels in Bulk by first selecting multiple cardholders to be modified, then

O. User Defined Fields
1. The System shall provide a minimum of 99 User Defined Fields for specific information about each access code holder.
2. User defined fields shall allow up to 50 characters per field.
3. The title of each field shall be programmable up to 20 characters.
4. There shall be a “Required” option for each user defined field that when selected forces the user to enter data in the user-defined field before the cardholder record can be saved.
5. There shall be a “Unique” option for each user defined field that when selected will not allow duplicate data from different cardholders to be entered.
6. There shall be a “UDF Data is Hidden” option for each user defined field that will require any given operator to have that option available in his/her password profile before that hidden data can be viewed.
7. Each User defined field shall have data masking in its setup that will require the data to be entered with certain character types in specific spots in the field entry window. This shall facilitate data to have like formatting display.
8. There shall be an option for each user defined field when selected will define the field as a deactivate date. The selection shall automatically cause the data mask to be formatted with the windows short date format. The system will order these fields and use the next future date of that order to set the deactivate date of that cardholder.
9. There shall be an option to select one of the 99 user defined fields as the Name ID. Data from this type of user-defined field will appear on the same window as the cardholder data entry window.
10. There shall be a search capability to allow any one user defined field or combination of user defined fields to be searched to find the appropriate cardholder.
11. String searches shall have the ability to be made on any field in conjunction with any other field searches.
12. The System shall have the ability to print cardholders based on and organized by the Used Defined Fields.

P. Code Tracing
1. The System shall perform Code Tracing selectable by cardholder and by reader.
2. Any code may be designated as a Traced Code with no limit to how many codes can be traced.
3. Any reader may be designated as a Trace Reader with no limit to which or how many readers can be used for Code Tracing.
4. When a Traced Code is used at a Trace Reader the Access Granted Message that usually appears on the Monitor window shall be highlighted with a different color than regular messages.
5. A short singular beep shall occur at the same time the highlighted message is displayed on the window.
6. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

2.7 APPLICATION SPECIFIC FEATURES

A. RS-232 ASCII Interface Specifications

1. The ASCII Interface shall allow for RS-232 connections to be made between the Host PC/Comm. Server and any equipment that will accept a RS-232 ASCII command strings such as CCTV switchers, intercoms and paging systems.
2. Each alarm input in the System shall allow for individual programming to output up to four unique ASCII character strings through two different Comm ports on the Host PC.
3. Each input shall have the ability to be defined to transmit a unique ASCII string for Alarm and one for Restoral through one Comm port and a unique ASCII string for a non-alarm abnormal condition and one for a normal condition through the same or different Comm port.
4. The predefined ASCII character strings shall have the ability to be up to 420 characters long with full use of all the ASCII control characters such as return or line feed. The character strings shall be defined in the database of the System and then assigned to the appropriate Inputs.
5. The Comm ports of the Host PC/Comm Server used to interface with external equipment shall be defined in the Setup portion of the software. The Comm port's baud rate, word length, stop bits, and parity shall be definable in the software to match that of the external equipment.
6. This RS-232 output shall be capable of connection to a pager interface that can be used to call a paging system or service and send a signal to a portable pager. The system shall allow an individual alphanumeric message per alarm input to be sent to the paging system. This interface shall support both numeric and alphanumeric pagers.
7. RS-232 used to transmit input alarms to central station automation software.
   a) The system shall be able to emulate the communications of a central station digital receiver to an alarm automation system. Thus allowing alarms that are received into the WinDSX system to be transferred to the alarm automation system just as if they were sent through a digital alarm receiver.
   b) The system shall be able to transmit an individual message from any alarm input to a burglar alarm automation monitoring system such as MAS or SIMMS.
   c) The system shall be able to append to each message a predefined set of character strings as a prefix and suffix.
   d) The system shall have the option of utilizing ACK and NAK messages from the automation system.
   e) The system shall have the ability to automatically clear alarms from its alarm queue after it has successfully transmitted it to the automation software.

****

Equipment needs for floor select elevator control will depend greatly on the number outputs required. Typical elevator interface will require one output per elevator cab per floor controlled. Some systems may require one additional output per elevator bank to place the elevators in after hours mode. Elevator travel cable may need to be installed for the elevator cab card reader to work.

****

B. Floor Select Elevator Control Specifications
   1. The Elevator Control function shall be an integral part of the Access Control System.
   2. The System shall be capable of providing full elevator security and control without any reliance on the Host PC for elevator control decisions.
   3. The System shall enable and disable car calls on each floor and/or floor select buttons in each elevator cab, restricting passenger access to the floors where they have been given access.
   4. The typical System shall utilize a card reader in each elevator cab.
   5. The System shall, through programming, automatically secure and open (un-secure) each floor select button of a cab individually by time and day. Each floor select button within a cab shall be separately controlled so that some floors may be secure while others remain open.

6. Once a floor select button is secure, it shall require the passenger to use their access code and have access to that floor before the floor select button will operate.
7. The passenger access code shall determine which car call and/or floor select buttons are to be enabled. This shall restrict the user from activating the floor select buttons corresponding to floors they not allowed access to.
8. The cardholder access shall be dynamic so that depending at which reader the access card is used determines which floor select buttons are enabled and shall prevent floor select buttons from being enabled in other elevator cabs.
9. The System shall enable the floor call buttons the cardholder has access to only in the cab where the cardholder used the card.
10. The System shall have the ability to limit an individual's access to specific floors at specific times per floor.
11. If the elevator System is so equipped, it shall be possible to receive a contact closure from the elevator equipment to indicate which call button is pressed.
    a) The contact closure shall connect to one of the alarm inputs on the Intelligent Controllers and could be used to record which call button the user pressed.
    b) The input from the intelligent controller shall have the ability to be used to reset any additional call buttons that may have been enabled by the users access code. This shall prevent "Tag-Along or Tailgaters" from pressing a call button that someone else's code enabled.
12. The floor select elevator control shall allow for manual override either individually by floor or by cab as a group from a workstation PC.
13. The system shall be capable of utilizing spare conductors in existing travel cable to connect the cab card reader through special line conditioning modules.

C. High Level Elevator Control Interface
1. Optionally, with the use of DSX-Soft I/O Software, the system shall have the ability to integrate with Elevator systems using a serial data connection instead of relay outputs. Instead of activating a relay output with a Code to Output Link it shall activate a virtual output that sends a unique command string to the elevator system telling it to enable a certain floor select button in a particular cab.

D. After Hours HVAC Control Specifications
1. The HVAC control features shall control and record the after hours use of the heating and cooling system in zones or tenant space.
2. This control shall give the administrator the ability to determine how much extra energy consumption each tenant is responsible for. This information can be used in billing tenants for the extra after hour usage.
3. At the specified time every day, the HVAC shall automatically go into its after hours mode. It shall then revert into its normal business hours mode by a tenant using an access code or card at a designated keypad or reader.
4. Once enabled, the tenant's HVAC zone shall be under thermostat control for a preset amount of time. When preset time elapses, the HVAC for that zone shall revert back to its after hours mode unless a tenant uses their code or card again. This shall continue until the unit automatically returns to its normal business hours operation.
5. The System shall allow the HVAC system to be enabled after a valid access in any of three ways;
    a) A range of 1 sec to 546 minutes (9.1 hrs) OR
    b) until the card or code is used again at the same or different reader/keypad.
    c) Until the system returns to its normal hours of operation.

    The HVAC control shall always allow for manual override from the PC.
6. Each of the outputs that control the HVAC zones shall allow control from up to four different time zones. The time zones shall allow for automatic control, based on time of day and day of week, including 3 unique holiday schedules.
7. The after hours HVAC control shall operate in conjunction with all other features running simultaneously and use the same PC that is controlling access for the building but shall not be reliant on the Host PC for any HVAC control decisions.

8. After hours HVAC control shall allow a reader or keypad to be used at each tenant space or in a common area shared by multiple tenants.

E. Real Time Guard Tour Specifications
1. Guard Tour shall be an integral part of the System.
2. A Tour Station is a physical Location a guard shall reach and perform an action indicating that the guard has arrived. This action, performed at the tour station, shall be one of 13 different events with any combination of station types within the same tour. A tour station shall be one of the following event types: Access Granted, Access Denied Code, Access Denied Card plus PIN, Access Denied Time Zone, Access Denied Level, Access Denied Facility, Access Denied Code Timer, Access Denied Anti-Passback, Access Granted Passback Violation, Alarm, Restoral, Input Normal and Input Abnormal.
3. Guard Tour shall allow proprietary (user controlled) direct connected Systems to make use of existing Access Control hardware to perform Guard Tour Management in a real time fashion.
4. Guard Tour and other system features shall operate simultaneously with no affect on each other.
5. The Tours shall be initiated at the PC.
6. Guard Tour shall allow the user to define specific routes or tours for the guard to take with time restrictions.
7. All guard tour activity shall be automatically logged to the computers Hard Disk.
8. The guard shall have a time window in which to reach every predefined Tour Station.
9. The guard, in making rounds, shall check in at predetermined Tour Stations within the specified times, otherwise an alarm shall be generated at the PC.
10. If the guard is late to a Tour Station, a unique alarm per station shall appear at the PC that indicates which station the guard failed to check in at.
11. If the guard is early to a station it shall be reported to the PC how early guard is.
12. The System shall allow the tours to be executed sequentially or in a random order with an overall time limit set for the entire tour instead of individual times for each tour station.
13. An optional user defined response plan shall be displayed for the operator or guard at the PC to follow should a "Failed to Check-In" Alarm occur.
14. There shall be 999 possible Guard Tour definitions with each Tour having up to 99 Tour Stations. All 999 Tours can be running at the same time.

F. Photo Badging Specifications
1. Photo Imaging shall be an integral part of the Access Control System.
2. The same software shall be configurable for Access Control only, Photo Badging only, or Access Control and Photo Badging.
3. The Number of badges shall be limited only by Hard Disk space.
4. The System shall have a true WYSIWYG badge building operation.
5. The System shall print on Paper or directly on Card Stock.
6. The Badge System shall operate in the same versions of Windows previously specified in this document.
7. The Badge System shall be LAN compatible.
8. The Badge System shall be a video based and film-less identification System.
9. The Badge System shall allow the user to issue access codes and at the same time generate an identification card, or badge, for temporary or permanent use.
10. The Badge System shall be a true Windows 32 bit application providing all of the advantages of the graphical user interface.
11. The System shall have a print preview capability.
12. The System shall have the ability to create different badge templates for each department, tenant, or contractor.
13. Templates shall be automatically selected for the card being printed based on the company or department the cardholder is assigned to.
14. The operator shall be able to override the automatic selection of the badge template and choose which template they want to use when creating a badge.
15. Badge backgrounds shall be selectable along with any other graphic images to be placed on the template.

16. Any of the cardholder information in the access System such as Name, Code, Company, Access Level, and any of the 99 User Defined Fields shall be selectable with the ability to place them anywhere on the card.
17. The System shall have the ability to Ghost an image or graphic with varying degrees of transparency to be placed anywhere on the card.
18. The System shall support unlimited usage of the 99 User Definable Fields that allow any data to be recorded and/or printed on a Photo ID badge.
19. The System shall include shapes that can be placed on the badge without having to use a draw program. The shapes shall utilize size and color capability of Windows.
20. Custom Text shall be able to be created in the imaging software, and placed anywhere on the card, utilizing full font, size and color capability of Windows.
21. Text shall be placed and optionally automatically centered within any region of the badge layout.
22. The System shall provide the ability to rotate to any degree text and barcodes on the printed badge.
23. The System shall facilitate printing multiple Bar Codes in 3 of 9 and 2 of 5 formats with Security Blocks, directly on the access card.
24. The System shall also have provisions to encode Magnetic Stripe cards as they are being printed with full integration to the database that shall provide the number to be encoded.
25. The System shall have provisions to print on both sides of a direct print card with only 1 pass through the appropriate printer.
26. The System shall have the ability to recognize a UDF field as an auto-incrementing card number. This will allow for each card to be printed with a unique number automatically generated by the software.
27. The System shall allow Batch Card Printing as follows: The System shall allow the cardholders to be selected using the normal Windows conventions for selecting multiple records from a list. It shall then print the badges from the selected list of cardholders using the correct template for each one.
28. The System shall have provisions to import captured images or photos using a digital camera. There shall be a quick and easy way to attach a secondary or digital camera to the System.
29. The System shall facilitate simultaneous connections to both a RGB output CCD Camera, and a digital camera.
30. The system shall support multiple images stored for each cardholder. Including signatures, portrait views, profile views, etc..
31. The System shall facilitate virtual Camera Pan and Tilt so that the camera does not have to be physically adjusted while capturing an image.
32. The System shall allow for the importing of the cardholder picture from a file.
33. The System shall allow for an image in a standard format to be imported and a copy of it saved in the format the System requires.
34. The System shall accept live video from any device providing an MCI or TWAIN interface that is Windows compatible.
35. The System shall allow multiple images on the same badge to include but not be limited to: Barcodes, Digital Photos, and Signatures.
36. The System shall support transparent backgrounds so the either a captured image photo or signature, is only surrounded by the intended background but not its immediate background.
37. The System shall facilitate the manual editing and cropping of the stored images. The System shall also have the ability to automatically edit the image and provide multiple views of the same image that have different characteristics and changes applied to each one for the operator to choose from.
38. The System shall have the ability to encode a Magstripe card in ABA Format on track 1, 2 or 3 at the same time the card is being printed.
39. The System shall be compatible with any Windows compatible direct card printer.
40. The System shall have an auto image retrieval feature that allows cardholder information and pictures to be automatically displayed on a PC running the same software.

41. The System shall support the automatic display of cardholder images on any or all selected readers when the cardholders use their card/code at the selected readers/keypads.
42. The System shall allow for a cardholder image to be recalled manually when the operator double clicks (selects) any access granted or denied event on the real time monitor window.
43. The System shall allow for automatic sizing of data fields placed on a badge to compensate for names that may otherwise be to large to fit in the area designated.

G. Visitor Assignment
1. The system shall have a means of allowing cardholders to be assigned with a visitor designation.
2. The system shall allow Names to be added that may or may not be assigned codes.
3. The system shall be able to restrict the access levels that may be assigned to cards that are issued to visitors.
4. There shall be an option on access levels that will designate an access level as visitor assignable.
5. The system shall utilize an online log book that during enrollment of a visitor the operator will have access to a search engine that will produce a view all names in the query and by point and click method enter the name of whom is being visited.
6. The system shall create an event for the history transaction as to the date time the visitor was added and to whom they were to visit.
7. Once a visitor is enrolled in the system upon the next visit the system shall allow the operator to recall that visitors' cardholder file and by utilizing the search engine query, point and click on the name of the person being visited on this occasion. The system shall create a transaction with visitors name and whom they were to visit on that date.
8. The system shall allow designation of any reader as one that deactivates the card after use at that reader, and logs to history as the return of the card.
9. The system shall have the ability to utilize the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

H. Time and Attendance
1. The System shall facilitate Time and Attendance using the access control hardware to gather the Clock IN and Clock OUT times of the users at designated readers.
2. Reports shall show IN and OUT times for each day, total IN time for each day and a total IN time for period specified by the user.
3. Reports shall have the ability to be viewed, printed, or saved to a file.
4. Reports shall have the ability to alpha sort on the persons last name, by Location or Location group.
5. Reports shall include all cardholders or optionally the ability to select individual cardholders for the report.
6. There shall be provisions for a real time display module (TDM) that is DC powered from the Access System Controller.
7. This TDM shall have a 7 segment LED display that is visible from all viewing angles. The segments shall be available in at least 1 inch and maximum of 5 inch height.
8. This Time Display Module shall be synchronized from the Access System Controller no less than once a minute. The TDM shall connect to the Access System Controller with a standard 4 conductor shielded cable and operate up to 500 feet from the controller.

I. Anti-Passback
1. The System shall have Global and Local Anti-Passback features by Location.
2. Synchronization of card IN/OUT status shall be global among up to 64 controllers, and shall not be dependent on the Host PC to be online for proper operation.
3. The System shall support Hard Anti-Passback. Hard Anti-Passback shall be defined as once a cardholder is granted access through a reader with one type of

designation (IN or OUT), the cardholder may not pass through that type of reader designation until the cardholder passes though a reader of opposite designation.

4. The System shall support Soft Anti-Passback. Soft Anti-Passback shall be defined as should a violation of the proper IN/OUT sequence occur access shall be granted, but a unique alarm shall be transmitted to the Host PC reporting the cardholder and the door involved in the violation. A separate report may be run on this event.
5. The System shall support Timed Anti-Passback. Timed Anti-Passback shall be defined as capabilities by a controller that shall prevent an access code from being used twice at the same device (door) within in a user defined amount of time.
6. The Anti-Passback schemes shall be definable for each individual door.
7. Anti-Passback override shall also be an option on a per card basis.
8. The System shall have the ability to forgive (or reset) an individual cardholder or the entire cardholder population Anti-Passback status to a neutral status.
9. There shall be a minimum of four different zones of anti-Passback that may be utilized within each Location. Each reader shall be assignable to 1 or all 4 Anti-Passback zones.
10. The four zones of Anti-Passback shall operate independently.
11. Controllers brought on line will have the anti-passback status of all users sent to them.

J. Live Video and Camera Control

1. The system shall provide means of displaying in a separate window the live video from a CCTV source.
2. The display window shall have separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan and minimum of two custom command auxiliary controls.
3. The command structure shall be such that one command string shall be issued when the control button is pressed down and another command shall be sent when the button is released. There shall be an option to automatically repeat the pressed down command as long as the button is pressed.
4. An Icon shall represent each camera to be controlled. Standard mouse clicking shall open a window that will display the video. If the system is connected to a video switcher it shall automatically send a command through a comm. port to display the requested camera when the Icon is selected.
5. The system shall provide a minimum of 7 Icons to represent different types of cameras. The ability to import custom Icons shall be provided.
6. The Icons shall be able to be placed on graphic maps to represent their physical Location. Standard mouse clicking shall open the display window for selected camera.
7. Each camera shall provide the ability to display and control a specific output on the video display window. The Icon representing the output shall display its real time status and respond in an animated fashion to the data reported from the field controller.
8. Each Input and Output shall be definable as associated with a camera. Upon selecting an Input or an output the system shall provide a pop up option window that will allow the camera associated with the point to be displayed.
9. The alarm-handling window shall have a command button that will allow the display of the camera associated with the alarm point.

****

Video capture card described below is an optional item, see hardware section or supplied by others.

****

10. The CCTV video shall be brought into a “Video Capture Card” installed on the PC where video is desired.
11. The system shall have a Next and Previous command buttons on the display window that when selected will allow the user to scroll through all cameras defined on a workstation.
12. The system shall provide that the same camera may be defined several times but display a different controlled Icon. This shall be used when one camera can view several entrances and will facilitate the use of the Next, Previous buttons.

3 EXECUTION

3.1 GENERAL REQUIREMENTS

A. Install system components and appurtenances in accordance with the printed instructions.
B. Provide all necessary interconnections, services, and adjustments required for a complete and operable system.
C. Install control signal, communications, and data transmission line grounding as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.

3.2 FIELD QUALITY CONTROL

A. Testing:
   1. Supply a proposed acceptance test procedure.
   2. Testing of system shall be the sole responsibility of the Contractor.
   3. Communications tests:
      a) Controllers to manager server.
      b) Manager server to client.
      c) Remote dial-up support.
B. Inspection:
   1. Provide an on-sight, factory-trained technician to assist, advise or manage installing personnel.
   2. All final connections shall be made under the direct supervision of the Systems Integrator.
C. Field Service:
   1. Provide first line support for both the hardware and software properties of the selected system.
   2. Provided second line support directly from the manufacturer for all component and computer hardware and all operating and application software that comprise the complete system.
   3. Determine and report all problems to the manufacturer’s customer service departments.
   4. Support shall be available to the integrator via the following methods:
      a) Phone inquiries.
      b) Direct dial-in to the customer system for remote system troubleshooting by a qualified Field Service Engineer.
      c) On-site visits if required, upon approval by the manufacturer's Customer Service Manager.

3.3 ON SITE COMMISSIONING AND TRAINING

A. The installing company shall provide direct participation in the on-site commissioning activity of new systems. Not less than 16 hours of on-site training shall be provided for a maximum of 6 representatives of Owner.
B. Provide systems administrator that is factory trained with the expertise on installing, configuring and commissioning the system to the customer’s specific requirements; and to provide on-site training on system operation and administration.
C. On-site shall be available for system administrators, Operators and other qualified personnel.
D. On site commissioning shall include:
   1. Hardware set-up and testing.
   2. Preventative maintenance and troubleshooting training.
   3. End User training.
   4. Database configuration and build assistance.

3.4 FINAL ACCEPTANCE

A. Perform the following performance standards before final acceptance:
   1. Operate all mechanical devices without down time for a period of 10 days.

2. Operate all electronic devices and equipment without downtime or programming problems for a period of 30 days.
3. Upon completion of system testing and before the acceptance cycle, provide 2 copies of system manual to Owner.

END OF SECTION