

- 3) The Software shall also be available preloaded on an NVR Server. This server shall be a preconfigured state-of-the-art Windows server ready to review and record video over the LAN and WAN (Internet).
- 4) Software shall provide full live digital video surveillance over a standard 100Base-T network by the use of a User Interface (UI) incorporating enterprise maps, site maps, navigation bars, user-configured URL links, and user-developed web pages.
- 5) The software shall support the simultaneous use of JPEG, M-JPEG, MPEG, H.264, and 1080P compression algorithm in the viewing of live video.
- 6) The software shall support the use of JPEG, M-JPEG, MPEG, H.264, and 1080P compression algorithm in the recording video.
- 7) The software shall offer network connectivity to other analog or IP family components that share all video and control data over the Ethernet network. The number of network-connected components is only limited to the number of assigned IP addresses.
- 8) The software shall support an unlimited number of IP devices and offer network connectivity to other family components that share all video and control data over the Ethernet network. The number of network-connected components is only limited to the number of assigned IP addresses.
- 9) The software, without any degradation to video quality, shall simultaneously offer on a single CPU:
 - a) IP continuous video playback.
 - b) IP video playback transmission to the Ethernet network.
 - c) IP continuous video receiving from the Ethernet network.
 - d) IP-channel continuous video playback running simultaneously with analog playback
 - e) IP video playback transmission to the Ethernet network running simultaneously with analog playback
 - f) A minimum of 32-Channel continuous video receiving from the Ethernet network running simultaneously with analog or IP playback
- 10) The recording server software shall operate on the following operating systems: Linux Suse 10 or RedHat Linux.

- 11) The UI server software shall operate on the following operating systems: Microsoft® Windows2000™ Server or Microsoft® Windows2003™ Server.
- 12) The networked system shall be comprised of:
 - a) The software platform.
 - b) Recording Servers (recorders).
 - c) Interface Servers (UI)
 - d) Clients (workstations)
- 13) The software shall offer features including the simultaneous display, playback, distribution and archive of multiple channel video. It shall collect multiple channels of analog and IP video and digitize them for the purpose of display, archive and requested distribution across the Ethernet network. Each channel of video data shall have the capability of being displayed, played back, distributed and archived simultaneously across several servers and clients across the network. The software shall also have full WAN and Internet capability, offering expandability beyond a corporate LAN.
- 14) Software shall support enterprise management of Roles and User accounts across all analog and/or IP solutions
- 15) Software shall support enterprise single user login to multiple sites, servers, cameras and maps without the need to re-authenticate.
- 16) Software shall support enterprise user authentication by user login and password, supporting varying roles by site.
- 17) Software shall be commercially available for purchase from an authorized distributor or dealer.
- 18) Recording Server shall be commercially available for purchase from an authorized distributor or dealer.
- 19) Interface Server shall be commercially available for purchase from an authorized distributor or dealer.

C. Hardware

- 1) Pre-configured Recording servers shall be available in, but not limited to the one or more combinations of the following features:

- a) Configurable frame rate by camera
 - b) Support 1 to “x” number of cameras, where “x” is determined by individual settings for
 - 1. Frame rate
 - 2. Compression
 - 3. Days of Storage
 - c) Support local recorded storage in the following configurations:
 - 1. 1U 500Gb to 1tb
 - 2. 2U 3Tb to 6Tb
 - 3. 3U 6Tb to 12Tb
 - 4. 5U 18Tb to 24 Tb
 - d) Support locally attached storage arrays:
 - 1. 3U 4Tb to 10.5Tb
 - 2. 4U 14Tb to 42 Tb
 - e) Support encoding servers:
 - 1. 3U, 1.5 Tb to 12Tb
 - f) Rack-mounted, full-height slots
- 2) Software shall operate on, but not be limited to, operating on all listed hardware.

D. Software

1) Installation

- a) The Software shall be available on CD-R format with complete installation documentation and provide a complete and comprehensive application for the operation and maintenance of the video surveillance system.
- b) Software shall be provided with technical documentation detailing system configuration files, including but not limited to,

default values, recommended settings, and narrative descriptions.

- c) Software shall not require manufacturer installation services or manufacturer-provided hardware to operate.
- d) Software shall be installable on systems operating with Microsoft® WindowsXP™ Professional, Microsoft® Windows2000™ Server, or Microsoft® Windows2003™ Server

2) Available Pre-Configured Modules

- a) Available pre-configured software modules shall include, but not be limited to:
 - 1. View Camera Listing By Site
 - 2. Infinite Matrix™ for simultaneous viewing of analog and/or IP cameras
 - 3. View Search Modules to research recorded video for either analog or IP cameras.
 - 4. Video Paging™ for the auto-display (without operator intervention) of cameras associated with alarms/alerts from system, or third party products
 - 5. Administrator functions, including but not limited to:
 - a) Role/Profile Management
 - b) User Account Management
 - c) Uploading of user HTML pages for site/user customization
 - d) Uploading of user Maps for site/user customization
 - e) Uploading of user logos/icons for site/user customization
 - 6. Off-Line Stored Segments for Creation, Deletion, Playback, and Download or Off-Line Segments
- b) Access to pre-configured software modules are controlled via system Profiles and User Account Management security.

3) Available Configurable Modules

- a) Available configurable software modules shall include, but not be limited to:

1. View Camera Listing By Site, Enterprise, or a combination thereof
2. View Any UI Map in Profile, including but not limited to, Site Map(s), Enterprise/District map(s), or Custom Map(s)
3. Include for use, any third party HTML page.
4. Include for use, any third party product that supports a web interface
5. Include for access, any link to a web page or product via link
6. Access to configurable software modules are controlled via system Profiles and User Account Management security.

4) Cameras

- a) System shall provide the following software functionality to include, but not be limited to:

1. A multiscreen display area that allows for screen displays of analog and IP cameras simultaneously:
 - a) Single camera.
 - b) Matrix views for 1, 4, 16, and 32 cameras
 - c) A multiscreen display area that allows for screen displays from cameras at multiple sites simultaneously.
 - d) User-defined matrix view, limited only by physical screen size
2. PTZ Controls. An operator shall be able to:
 - a) Control pan, tilt, zoom, iris and focus.
 - b) Execute preset positions.
3. User selectable resolution for analog cameras shall include capture sizes of:
 - a) 320 x 240 pixels
 - b) 640 x 480 pixels
 - c) 704 x 480 pixels
 - d) 1080P

- e) User selectable resolution for IP cameras shall be configurable to the supported IP camera resolution.
 - 4. The software shall permit the viewing of live or recorded video from any workstation on the network that has access to any recorder on the network.
 - 5. Software shall support, at a minimum, the following stationary and PTZ cameras:
 - a) Analog NTSC
 - b) Cisco
 - c) Axis
 - d) Sony
 - e) Panasonic
 - f) Toshiba
 - g) Linudix
 - h) D-Link
 - 6. Software shall incorporate, without re-installation or upgrade, additional cameras with the addition of camera script files, which define camera behavior.
 - 7. Manufacturer shall provide additional camera scripts upon request at no charge.
- 5) Speed
- a) All units shall be able to record up to 30 fps per camera for analog cameras.
 - b) All units shall be able to record up to 30 fps per camera for IP cameras, should the IP camera support such a transmission rate.
- 6) Video Retrieval
- a) Video retrieval shall be performed by:
 - 1. Selecting the camera and recorded date desired
 - 2. Selecting from a "calendar-style interface", the hour to be retrieved
 - 3. Selecting the minute within the hour to be reviewed via image thumbnail or minute link

4. Playback shall allow for play, reverse, and frame-by-frame functionality.

7) Alarms/Alerts

- a) Units shall support, but not be limited to, alarm input via:
 1. External Alarms via dry contact closure for both analog or IP cameras
 2. Camera alarms shall include but is not limited to:
 - a) Video Motion Alarms
 - b) Video Loss Alarms.
 3. Third-party alarm conditions received via TCP/IP transmission protocol or HTTP post.

8) Configuration Files

- a) Software configuration files shall be stored in non-proprietary XML or text format and shall include, but not be limited to:
- b) Camera configuration files shall include, but not be limited to:
 1. Camera name
 2. Live Camera Viewing Resolution
 3. Camera Playback Viewing Resolution
 4. Image storage location (IP cameras)
 5. Internal IP and port address
 6. External IP and port address
 7. Retention days for recorded video
 8. Username for camera
 9. Password for camera
 10. Notification or alarms/alerts
 11. Motion detection
- c) System Profile files shall include, but not be limited to:
 1. Profile name
 2. Allowed devices, including cameras
 3. Allowed software modules, including, but not limited to:
 - a) Pre-Configured Software modules

- b) Configurable Software modules
 - c) Map UI files
 - d) User configured web pages
 - e) User configured web links
- d) User account files shall include, but not be limited to:
1. User name, first and last
 2. User ID
 3. Password (encrypted or text)
 4. User configured navigation bar logo/icon
 5. User profile
- e) Video Paging configuration files shall include, but not be limited to:
1. Alert/alarm device ID
 2. Related Camera Name for auto-display
 3. IP address on which to listen for 3rd party alarm/alert message
 4. Port on which to listen for 3rd party alarm/alert message

9) Authorization Rights

- a) Authorization rights setup shall be performed using the Profiles and Users screens.
- b) Profile rights shall be available to configure, by specific site. Profile functionality shall be as follows:
1. Ability to establish unique Profile name by Site.
 2. Ability to create a unique alphanumeric Profile name.
 3. Ability to include specific system devices in that Profile. System devices can include, but are not limited to, analog cameras, IP cameras, alert devices, alarm devices.
 4. Ability to include specific software modules, web pages, and access links to other web-enabled products.
 5. Ability to assign Profiles to a user ID to control user access to devices, software modules, web pages, and access links.

c) User rights shall be available to configure, by specific site. Use functionality shall be as follows:

1. Ability to establish unique user ID name by Site.
2. Ability to create a unique alphanumeric user ID
3. Ability to store user information such as first name and last name per user ID.
4. Ability to assign a Profile to a user ID
5. Ability to assign a unique graphic to each user ID to be displayed in the navigation panel of that user IDs UI.

d) Profile rights shall not be restricted to require inclusion of camera or alarm/alert devices.

e) System shall allow use of Profile and User rights to control access to web pages and access links without requiring inclusion of camera or alarm/alert devices thereby providing portal functionality unrelated to physical security devices.

f) There shall be no virtual limit on the number of Profiles and Users that can be authorized in the software, either centrally or at the Site level.

E. Client Workstation

- 1) Access to all users UI shall be via web interface and shall not require the installation of client software on an end-user workstation.

F. Converged Solution

1) Integrated Products

a) The Software shall be integrated with the following products:

1. VSS Steel: Access Control/Intrusion Detection
2. MC Dean Security ACES: Access Control/Intrusion Detection
3. Status Solutions: Notification
4. IPCelerate: Paging and Notification

b) The Software shall be able to provide Video Pages in response to notifications from third party products that conform to published messaging protocols.

c) APIs shall be pre-installed and available for use at no charge.

2) Alerts/Alarms/Triggers

a) The Software shall have the capability to execute Video Pages to a user's workstation in response to alerts, alarms, and triggers.

3) Cisco CallManager

a) The Software shall have the capability to provide images to be displayed on Cisco IP phones that support display of images.

4) 3rd Party Products

a) The Software shall have a documented communication protocol that can be utilized to enable Video Paging without modification of Software or custom development by manufacturer.

b) The Software shall be able to integrate with the following recording servers:

1. VSS Alloy IP or Analog Servers
2. Cisco Systems, Video Surveillance Media Servers
3. Chance-i, DVR
4. Dedicated Micros, DVR and DM Sprite series
5. Pelco, Endura Products
6. Progressive Systems/LenSec, DVR
7. Any third-party video product with a published API that conforms to open-standard architecture

G. Acceptable Product

1) The Converged IP Video Management System shall be the VSS Alloy Appliance Server.

H. Service and Support

1) Remote Service

a) Vendor shall provide daily system checks to include but not limited to:

1. Visual verification of unobscured camera images. Automated systems are not acceptable.
2. Verification that cameras are recording as defined.
3. Verification of operation of all alert and alarm devices
4. Verification of proper functional operation of video server or alert/alarm server
5. Verification of proper functional operation of video paging components

2) Notification

a) Vendor shall provide same-day notification of any system and/or device outages including but not limited to cameras, video servers, analog-to-IP converters, alert/alarm servers, alert devices, and any ancillary equipment integrated into the proposed solution related to physical security.

b) Vendor shall provide dispatch of a local technician to site to address outages of any physical security devices.

c) Vendor shall provide a response schedule for outages.

I. Staff

1) All on-site and remote staff shall be required to provide a life-time national criminal background check with no felony convictions. Misdemeanors will be reviewed for approval. Staff includes, but is not limited to:

- a) On-site installation crews
- b) On-site maintenance and service staff
- c) Remote maintenance and service staff
- d) Any manufacturer representative that may provide support for the proposed solution
- e) Sales and management representatives for vendor
- f) Customer reserves the right to request the above-described background check from the Vendor for any personnel that Vendor wishes to access, review, or discuss the implemented solution

- 2) Background checks are to be submitted annually and at the Customer request.
- 3) Vendor shall have at a minimum the following qualifications/certifications:
 - a) Cisco Authorized Technology Provider for Physical Security
 - b) VSS Authorized Dealer or Authorized Installer
 - c) Dell Server Repair Certification
 - d) Dedicated Micros Reseller and/or Development Partner
 - e) Axis Reseller and/or Development Partner
 - f) Cisco Certified CCNA, CCDA, or CCNP on staff and assigned to account
 - g) Hold a security license for the jurisdiction of the installation

ACCESS CONTROL/INTRUSION DETECTION

PART 1- GENERAL

1.1 SYSTEM DESCRIPTION

The Contractor shall provide a Security Management System (SMS) consisting of an Access Control System (ACS), Intrusion Detection System (IDS). The SMS shall also provide seamless CCTV integration with existing video surveillance systems.

The SMS shall be the key central component for managing physical security and the bridge between physical and logical security for this project. The system shall provide a variety of integral functions including the ability to regulate access and egress; provide identification credentials; monitor, track and interface alarms; and view, record and store digital surveillance video.

1.2 SECTION INCLUDES

VSS Alloy Appliance Server

1.3 DEFINITIONS

- A. No Substitutes: The exact make and model number identified in this specification shall be provided without exception.
- B. Or Equal: Any item may be substituted for the specified item provided that in every technical sense, the substituted item provides the same or better capability and functionality

- C. Or Approved Equal: A substitute for the specified item may be offered for approval by the Owner. The proposed substitution must, in every technical sense, provide the same or better capability and functionality as the specified item. Such requests for approval shall be submitted for approval and must be obtained within the time frames outlined.

1.4 SECURITY MANAGEMENT SYSTEM

The SMS shall be able to seamlessly interface with and monitor intelligent system controllers, reader interface modules, input modules, output modules and peripheral devices approved for use by the SMS manufacturer. The system shall be able to manage up to 25,000 cardholders, up to 512 card readers, 4096 inputs, 406 outputs and 512 zones per site.

1.5 SYSTEMS NETWORKS

The SMS shall be able to communicate with intelligent system controllers via RS-485, RS-232, TCP-IP/Ethernet and Dial-up via Modem. All tasks shall be accessible from any compatible client workstation on the network utilizing traditional client server or peer to peer architecture.

The SMS shall utilize an open architecture where all data must reside on a single database and must be accessible in real time to every/any SMS workstation connected to the network.

1.6 ENTERPRISE SOLUTION

The SMS shall be capable of managing multiple sites from a single enterprise client. Upgrades or expansion of the SMS to a larger size system in scale shall not require installation of a different and or new SMS application or require the administrator/operator to learn a different and or new interface from the previous version.

1.7 FIELD EQUIPMENT

Field equipment shall include intelligent modules, sensors and controls. Local processors shall serve as an interface between the SMS and sensors and controls. Data exchange between the SMS and the local processors shall include down-line transmission of commands and software and databases to local processors. The up line data exchange from the local processor to the SMS shall include status data such as intrusion alarms, status reports and entry control records. Local processors are categorized as intelligent controllers, alarm annunciation, entry control or a combination thereof.

PART 2- PRODUCTS

2.1 ACCEPTABLE MANUFACTURER

- A. VSS (Vision Security Software), 2200 Market Street, Suite 305, Galveston Island, TX, 77550, USA Telephone: 409.763.6323, Fax: 678.868.4009 Email: info@vssc corp.com, Internet: www.vssc corp.com
- B. Substitutions: Not Permitted

2.2 MATERIAL REQUIREMENTS

- A. Units of equipment that perform identical, specified functions shall be products of a single manufacturer. All material and equipment shall be new and currently in production. Each major component of equipment shall have the manufacturer's model and serial number in a conspicuous place. System equipment shall conform to UL 294 and UL 1076.

2.3 HARDWARE

- A. The SMS shall provide the necessary hardware to monitor alarms and events throughout a facility, arm and disarm alarm zones, and manage access granted/denied decisions.

2.4 INTELLIGENT MODULES

- A. Intelligent Modules (IM=s) define the components that interface with access control readers, door hardware and intrusion detection devices. Intelligent Modules shall include the following configurations:
 - a. Intelligent Reader Module (IRM): supports up to 2 readers, 8 supervised inputs, 4 auxiliary outputs.
 - b. Intelligent Input Module (IIM): supports up to 16 supervised inputs, 4 auxiliary outputs
 - c. Intelligent Output Module (IOM): supports up to 16 auxiliary outputs, 4 supervised inputs

- B. The IM's shall provide full distributed processing of all access control and alarm monitoring operations. Access levels, time zones, holiday groups, ID cards, reader, input and output configurations shall be downloaded to each IM. All access granted/denied decisions must be made at the IM, based on reader location, cardholder identification, time of day and day of the week. Systems that use reader modules at the door and store data at a remote controller are not acceptable.
- C. Each IM shall provide fast responses to reader transactions, allowing doors to be unlocked within 100 msec regardless of volume of card activity or size of cardholder database.
- D. Each IM shall utilize a high-speed microprocessor-based chip capable of communicating with the Host PC at speeds of up to 115200 bps. Baud rates shall be adjustable at the PC, immediately altering the communication speed of all IM=s on a communication line to the selected rate. Systems that require field technicians to adjust individual panel settings through dip switches, rotary switches, jumpers or field programming devices are not acceptable.
- E. The IM=s shall utilize pluggable, replaceable, hot-swappable daughterboards for RS232, RS485 and TCP/IP module communications. The following communication protocols shall be supported:
 - a. RS232 at speeds of up to 115.2Kbps, direct connection or dial-up modem
 - b. RS485 full duplex at speeds of up to 115.2Kbps
 - c. TCP/IP at speeds of up to 10 Mbps (RJ45 10Base-T)
- F. Communication daughterboards shall incorporate extensive transient voltage protection on the board and provide individual transmit and receive LED=s.
- G. Each reader port shall support multiple reader types and technologies including Wiegand, card & pin, proximity, biometric, smart card, magnetic stripe and bar code. Individual control of red & green LED=s and sounder shall be provided by the IM, as well as extensive transient voltage protection on the board. Reader power shall be provided by the IM at 12VDC @ up to 200ma per reader.
- H. Each input point shall be individually programmable for 2-, 3-, or 4-state supervision and shall incorporate extensive transient voltage protection on the board. Each input point shall differentiate between ANormal@, AAlarm@, AShort@ (tamper), and/or AOpen@ (trouble) conditions. Systems that require an additional input point to produce 4-state alarm reporting are unacceptable.

- I. Each outpoint shall be a Form AC@ relay with outputs rated at 1 amp at 24VDC each with its own individual LED and shall incorporate extensive transient voltage protection on the board.
- J. All power and wiring for the card reader and alarm network shall be distributed from within the IM's enclosure using quick disconnect terminal blocks. The enclosure shall be construction of 16 gauge steel for durability and shall include knockouts, a hinged cover, key lock, tamper switch, power supply and a self-contained replaceable battery backup.
- K. The IM power supply shall be provided with LED indicators for normal operating condition and loss of AC and/or DC output and stand-by battery supplying power. Battery leads, built in charger for sealed lead acid or gel type battery and automatic switchover to stand-by battery if AC fails are to be provided as standard.
- L. The IM's must utilize an advanced auto-recognition and auto-configuration mode for automatically detecting, programming and downloading required data to each module. Auto-recognition and configuration information shall include: communication type, module type, address, baud rate, memory size, and all required operational data. Systems that require manual entry of module configuration and data shall be unacceptable.
- M. The IM's shall incorporate AFLASH@ memory technology for remote upgrades to all module firmware. Systems that require field technicians to upgrade by replacing EPROM's are unacceptable. Firmware must be downloadable to all IM's simultaneously. Systems that require individual downloading of firmware to field devices are not acceptable.
- N. The IM's shall be of a modular design and all address and baud rate settings shall be auto-configured and auto-detected without the use of rotary switches, dip switches, jumpers or other wiring. System components that require rotary switches, dip switches, jumpers or field programming devices to set address and baud rate are not acceptable.
- O. Each IM shall be capable of storing over 26,000 cardholders at the door. Systems that use reader modules at the door and store data at a remote controller are not acceptable. All required data files shall be automatically downloaded to all appropriate modules. When changes are made to the data files, the Host PC shall automatically download those changes to all affected modules only. Each IM may have a different set of cards appropriate to its assigned readers and access levels for maximum utilization of memory.

- P. All alarm and card activity shall be time-stamped at the IM and shall have a throughput of cardholders not to exceed 100msecs. Systems that process cardholder transactions at a master controller versus locally at the door are not acceptable.
- Q. Each IM must offer simultaneous support of multiple reader types and technologies including up to 29 different card formats containing up to 64 bits of data each.
- R. Buffer capacities shall be user-definable on a per module basis, dynamically adjusting the number of alarms, transactions and commands stored in memory while waiting to be transferred to the Host PC.
- S. All communications between the module and the primary PC shall be supervised and allow user-defined alarm generation in the event of communication failure. The module shall buffer all activity that occurs during a loss of communication. Once re-established, the module will automatically upload all buffered activity, alarm and command data to the primary PC.
- T. In the event that a module's data tables are damaged or destroyed, the module shall automatically request a download of all necessary data, without requiring any operator intervention.
- U. The IM must be able to support local, hard, soft and timed anti-passback and door control functions, even if off-line from the system's central PC.
- V. It shall be possible to share door control devices such as contacts, REXs and output relays when using two readers (in/out) at the same door.
- W. Every input and/or output available on the IM may be used for any appropriate system function. Systems that dedicate specific inputs and outputs for door control are not acceptable.
- X. Each IM shall contain a replaceable lithium ion battery for protection of the on-board data for at least two months of internal memory retention if there is no external power source.
- Y. Upon loss of AC power, each IM shall have a battery backup that provides for up to [four (4), eight (8), twelve (12)] hours of continuous operation. It shall be possible to generate and report an alarm in the event of loss of AC or low battery conditions.
- Z. Up to 32 IM's of any combination (IRM, IIM, IOM) may be configured on a single communication line.

AA.Up to eight (8) communications lines may be defined on a single system.

2.5 SERVER/WORKSTATION

- A. The SMS server/workstation shall be standard, off the shelf, unmodified digital computer of modular design.
- B. Each server/workstation shall meet the following requirements, at a minimum:
 - a. Pentium IV 1.6GHz Dual-core Processor or greater
 - b. 1GB RAM or greater
 - c. 21" Monitor, .28 dot pitch or better with built-in touchscreen capability
 - d. Standard AWindows@ compatible keyboard & mouse
 - e. 80GB Hard Drive or greater
 - f. 48X read CD ROM drive
 - g. Video board capable of displaying 32-bit true color at a screen density of 1280 x 960, or better
 - h. USB2.0 ports adequate for reporting requirements
 - i. 16-bit sound card with associated speakers
 - j. 100 auto-sensing NIC
 - k. Operating system shall be Windows Vista or greater
 - l. True On-Line UPS shall be provided

2.6 PRINTERS

The system shall support any standard AWindows-compatible@ printer for reporting and badging, provided the printer manufacturer supplies a Windows print driver.

2.7 READERS

The SMS shall support multiple reader types and technologies from any manufacturer that utilizes industry standard Wiegand output of up to 64 bits. Supported reader technologies

include, but are not limited to prox, keypad, prox/keypad combo, bar code, magnetic stripe, smart card and biometric devices.

2.8 INPUTS

The SMS shall support any industry-standard input devices including, but not limited to, magnetic door contact switches, request to exit devices and tamper switches.

2.9 OUTPUT RELAYS

The system shall support any industry-standard output device including, but not limited to, door locking devices, annunciators, and lights.

2.10 SOFTWARE

The SMS software shall be a true 32-bit, multi-tasking, multi-user application, compatible with Windows Vista operating systems. The system must utilize a single seamlessly integrated database for all system functions, capable of supporting the Primary server/workstation and up to 32 administration/monitoring workstations per system. The system shall be modular in design, allowing for ease of future upgrades and enhancements.

2.11 SOFTWARE FEATURES

- A. The software shall utilize standard AWindows@ design features such as task pane, minimize/maximize, close buttons etc. Standard AWindows@ navigation features such as point and click, drag and drop, and relocation of windows shall also be supported.
- B. The software shall be specifically designed to allow users to perform administrative and monitoring functions using their finger on a touch sensitive screen, rather than with a keyboard and mouse.
- C. Each window shall provide simple easy to follow instructions and/or descriptions of the features and options available for operation selection or definition.
- D. The software shall utilize an integrated text-to-speech engine providing audible feedback to operators for prompts, descriptions and actions.
- E. Each authorized system operator shall be assigned an ID number, password and user-defined system access level in order to Alogon@ to the system. It shall be possible to define an unlimited number of system access levels capable of limiting operator access to sensitive information. It shall be possible to permission protect every major feature and function in the system.

2.12 SYSTEM ADMINISTRATION

2.12.1 HARDWARE CONFIGURATION

- A. The SMS shall support up to eight (8) COM ports, utilizing RS485, RS232, TCP/IP or dial up connections. Each communication port shall be separately configured for the following:
 - a. User-defined descriptive name
 - b. Port number
 - c. Baud rate (2400 to 115200), parity, data bits and stop bits
 - d. Dial-up parameters to include dial string, number of sections to wait for a connection before and after dialing, consecutive redial attempts, buffer capacities, alarm priority and events requiring dial-up activation.

- B. The SMS shall allow the administrator to add, edit or delete communication line configurations and descriptions. Each communication line shall be capable of supporting up to: 32 IM=s, 64 readers, 512 supervised inputs and/or 512 auxiliary outputs. Each communication line shall be separately configured to include the following:
 - a. User-defined descriptive name
 - b. COM port assignment (hardwired or IP)
 - c. Polling frequency and delay
 - d. Communication line down alarm information to include alarm priority (0-255), operator response requirement before clearing, and associated instructions and responses.

- C. A system status window shall be available and displayed from any workstation for diagnostics, troubleshooting and manual control of communications to Intelligent Modules.

- D. The system status window shall indicate, in real-time, the number of communication ports defined, the status of the communication line, the quantity, address and type of IM's connected to the line and the status of each IM. Systems that utilize a tree configuration to display system status shall not be acceptable.

- E. Status indicators shall be color-coded to indicate the following: Gray (communication line not defined); Green (communication line/module on line); Red (module off-line), Blue (module receiving download), Black (module in maintenance mode), Yellow (new module detected). Systems requiring field verification of communication line and module status shall not be acceptable.

- F. From the system status window, it shall be possible to update/send configuration and status information to each individual IM. Available commands shall include the following:
 - a. Validate module status
 - b. Send date and time
 - c. Flush alarm, command and/or transaction buffers
 - d. Clear all ID card anti-passback statuses
 - e. Reset the controller
 - f. Send keypad commands
 - g. Download firmware, custom configuration files, card formats, reader, inputs and output information, keypad commands, ID cards, holidays, time zones and access levels

- G. The system status window shall support an advanced auto-recognition and configuration feature for detecting all IM=s on a communication line. From this window, the system shall continuously query all defined communication lines and automatically detect the presence of all new modules. Upon detection, the system shall immediately add the module to the appropriate communication line and assign it the detected module type and next available address.

- H. In addition to system hardware, the status window shall also provide workstation statistics to include CPU speed and percent being utilized, installed memory and percent being utilized and hard drive size and percent being utilized.

- I. The system status window shall support the configuration of IM's and associated devices before, during or after they are physically installed. After a module has been auto-detected, the auto-detected module may be changed to any pre-defined module, assuming all of it=s settings and data tables by using a simple Adrag-and-drop@ process. Auto-detected modules may also be manually edited and customized for system operation.

- J. The SMS shall allow the administrator to swap the identities of two configured modules, automatically exchanging the addresses, settings and data tables between the two modules.

- K. The system shall allow the administrator to define standard default configurations for each IM. These default profiles shall serve as a model for all field devices such as readers, inputs and outputs, connected to the system. Each module type shall have it=s own default profile. As IM=s are added to the system, by auto-detection or by manual data entry, the default profiles may be automatically applied to the module=s configuration.