Maxxess eFusion A&E Specification

Version 1.9

January 1, 2022

ABSTRACT

eFusion Application Architectural and Engineering Specifications
SECURITY MANAGEMENT SYSTEM

SECTION 28 10 00
ACCESS CONTROL SYSTEM

PART 1 GENERAL

1.01 SUMMARY

A. This section provides a description of a Security Management System (SMS) that includes software and hardware for physical access control, and integrates with optional video surveillance and intrusion detection system software and hardware.

B. Related Sections

1. Section 08 71 53 – Security Door Hardware
2. Section 28 05 00 – Common Work Results for Electronic Safety and Security
3. Section 28 16 00 – Access Control Interfaces
4. Section 28 17 00 – Access Control Identification Management Systems
5. Section 28 20 00 – Video Surveillance
6. Section 27 05 28 – Pathways for Communications Systems
7. Section 27 10 00 – Structured Cabling
8. Section 27 15 00 – Communications Horizontal Cabling
9. Section 28 13 43 – Access Control Identification Management Systems
10. Section 28 23 00 – Video Management System
11. Section 28 31 00 – Intrusion Detection

1.02 REFERENCES

A. Abbreviations and Acronyms

1. AES: Advanced Encryption Standard.
2. ANSI: American National Standards Institute.
3. API: Application Programming Interface.
4. AWG: American Wire Gauge.
5. SMS: Security Management System.
6. IEC: International Electrotechnical Commission.
7. IEEE: Institute of Electrical and Electronics Engineers.
8. IP: Internet Protocol.
9. ITU: International Telegraph Union.
10. NOC: Network Operations Center.
11. OPC: Open Platform Communication.
12. OSDP: Open Supervised Device Protocol.
13. PACS: Physical Access Control System.
14. PII: Personally Identifiable Information.
15. PIN: Personal Identification Number.
16. SaaS: Software as a Service.
17. SIA: Security Industry Association
18. SIP: Session Initiation Protocol.
19. SNMP: Simple Network Management Protocol.

20. SSL: Secure Socket Layer.
21. TCP: Transmission Control Protocol.
22. TIA: Telecommunications Industry Association.

B. Definitions

1. Access Control: A function or a system that restricts access to authorized persons only.
2. Anti-Passback: An access control security measure to prevent or discourage a cardholder from allowing another individual to use the cardholder's card to gain entry to an access-controlled area immediately after the cardholder gains entry, without the cardholder first exiting the area. Enabling Hard and Soft Anti-Passback requires that each door providing entry into the restricted area have two readers, one outside the area (referred to as an Entry Reader) and one inside the area (an Exit Reader).
    a. Hard Anti-Passback: Prevents a card from being used twice in a row to gain entry to the same area. Once a cardholder presents a card and gains entry, the card may only be used to exit the area, and until the card is used to exit the restricted area, other entry attempts using the card will be denied. Use of the card to attempt entry into any other areas will not be successful until it has been used to exit the area previously entered.
    b. Soft Anti-Passback: Grants access for all valid authorized card presented at an access-controlled area regardless of the card already having been used for entry; however, upon successive entry events the system also generates an Anti-Passback Violation event, providing notice that the Anti-Passback security policy has been violated**.** The occurrence of an Anti-Passback Violation means that an unauthorized person may have gained access to the restricted area.
    c. Timed Anti-Passback: An Entry Reader only is used at each door of the restricted area. Since there is no Exit Reader, a time limit is specified for the Anti-Passback policy to be applied on a per-user basis**.**
3. API: Application Programming Interface, a set of clearly defined methods of communication between various software components.
4. Authentication: A process that verifies the origin of information, or determines an entity's identity.
5. Authorization: A process that associates permission to access a resource or asset with a person and the person's identifier(s) for the purpose of granting or denying access.
6. Auto-Relock: Door control feature that automatically relocks the door after access has been granted and the door has opened and closed, regardless of the time allowed for the door to momentarily remain unlocked to allow entry.
7. Biometric: A biometric is a unique identifying physical or physiological characteristic of an individual that can be used to identify that individual.

Examples include, but are not limited to DNA, fingerprint, gait, face recognition, hand geometry, iris recognition, palm print, palm veins, retina and voice.

8. Central Station: A central alarm monitoring station service providing its subscribers with around the clock real-time alarm monitoring and response services by trained operators and alarm investigators.
9. Credential: Data assigned to a person and used to identify that person or entity. The data may be printed on an access/ID card, such as a photograph, name, and other printed data, or stored electronically in the computer chip on a smart card, an RFID chip, or in the memory of a biometric reader.
10. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual.
11. Intuitive: A software application is intuitive when users understand its behavior and effect without use of reason, experimentation, assistance, or special training.
12. OSDP: Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products, and uses RS-485 data communication.
13. PACS: Physical Access Control System
14. PSIM-Capable: Of an access control and alarm monitoring system, having many points of basic PSIM functionality, so that, with the addition of optional applications and integrations, provides a full set of situational awareness and situation / event / incident response capabilities typically only found in a major PSIM application.
15. RS-232: ANSI/TIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.
16. RS-485: ANSI/TIA standard for multipoint communications.
17. TCP/IP: Transport control protocol/Internet protocol.
18. Wiegand card: An access control credential card that uses the Wiegand effect to magnetically treat wires embedded in the card to retain a numerical code that can be read by Wiegand-effect card readers. Wiegand cards conform to the ISO/IEC 7810 D-1 size and thickness specifications.
19. Windows: Microsoft® Windows®, a computer operating system by Microsoft Corporation.
20. Workstation: A network-connected personal computer intended to be used by a specific person or people for the performance of specific tasks, such as alarm and video monitoring. ID badge issuance or visitor registration.

21. X.509: A standard for a public key infrastructure (PKI) to manage digital certificates, public-key encryption and public key management.

C. Reference Standards

1. Department of Justice American Disability Act (ADA)
    a. 28 CFR Part 36 – ADA Standards for Accessible Design 2010
2. Federal Communications Commission (FCC):
    a. FCC Part 15 – Radio Frequency Device
    b. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network
3. Federal Information Processing Standards (FIPS):
    a. FIPS 197 – Advanced Encryption Standard (AES)
4. Institute of Electrical and Electronics Engineers (IEEE)
    a. IEEE 802.3 – Ethernet standards
5. International Organization for Standardization (ISO):
    a. 11801 – Generic Cabling Standard
6. ITU Telecommunications Sector (ITU-T)
    a. X.509 – A framework for public key infrastructure (PKI) and privilege management infrastructure (PMI)
7. Security Industry Association(SIA):
    a. ANSI/SIA CP-01-2014 – False Alarm Reduction Standard
    b. OSDP v2.1.5 – Open Supervised Device Protocol
8. Telecommunications Industry Association (TIA):
    a. ANSI/TIA-568 – set of telecommunications standards:
    b. ANSI/TIA-568.0-D – Generic Telecommunications Cabling for Customer Premises
    c. ANSI/TIA-568-C.0 – Generic Telecommunications Cabling for Customer Premises
    d. ANSI/TIA-568-C.1 – Commercial Building Telecommunications Cabling Standard
    e. ANSI/TIA-568-C.2 – Balanced Twisted-Pair Telecommunications Cabling and Components Standard
    f. ANSI/TIA-568-C.3 – Optical Fiber Cabling Components
    g. ANSI/TIA-569-D – Telecommunications Pathways and Spaces
    h. ANSI/TIA-606-B – Administration Standard for Telecommunications Infrastructure
    i. ANSI/TIA-607-C – Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises
    j. ANSI/TIA-232-F – Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

k. ANSI/TIA-422-B – Electrical Characteristics of Balanced Voltage Digital Interface Circuits
l. ANSI/TIA-485-A – Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

9. National Institute of Standards and Technology (NIST)

a. FIPS 140-2 – Security Requirements for Cryptographic Modules, including the use of X.509 public key infrastructure (PKI) digital certificates
b. FIPS 197 – Advanced Encryption Standard (AES)
c. FIPS 201 – FIPS 201-1 and FIPS-201-2 standards – Personnel Information and Verification (PIV) standards for Government Agencies, including PIV, PIV-II and CAC cards

1.03 QUALITY ASSURANCE

A. Manufacturer shall be capable of providing field service representation during construction, approving acceptable installer and approving application method.

PART 2 PRODUCTS

2.01 MANUFACTURER

A. Maxxess Systems, Inc.

1. 22661 Old Canal Rd, Yorba Linda, CA 92887

a. Telephone: (714) 780-7458
b. Website: https://www.maxxess-systems.com

2.02 PRODUCT SUBSTITUTIONS

A. No product substitutions permitted.

2.03 SECURITY MANAGEMENT SYSTEM (SMS) OVERVIEW

A. SMS shall consist of compatible software and hardware designed to work together to provide a software and hardware system platform that can be configured to meet the user's unique security management needs.

1. *Scalability:* Support small two-reader access systems up to large, multi-building, multi-site enterprise level systems supporting an unlimited number of doors and card holders using a single suite of software.

2. *Architecture:* Have a client-server architecture that includes system server software, thin client applications for user workstation functionality, and mobile applications ("apps") for use on personal mobile devices.

3. *Modular Configuration:* Provide configurable functionality to meet the user's unique needs by mixing and matching functional software modules, approved

security hardware devices, personal computer workstations, and personal mobile devices. Available software modules shall include:

a. Access Control.
b. Alarm Management & Reporting.
c. Interactive Graphical Floorplans.
d. Report Generation.
e. MX+ Browser-based Interface.
f. Optional InSite Module
g. Optional Elevator Control.
h. Optional ID Badging.
i. Optional On-site Cardholder Time & Attendance Reporting.
j. Optional Auto Import/Export.
k. Optional Video System Integration.
l. Optional Database Integration Service.
m. Optional Guard Tour.
n. Optional Asset Management.
o. Optional Building Controls Software Integration.
p. Optional Visitor Management.
q. Optional 3rd Party System Integration.
r. Optional Personal Security and Productivity.
s. Optional Mobile Identification and Verification.

4. *Reliability:* Manufacturer shall be a global company whose core business has been the design, production, and distribution of security management products for over 20 years, and has deployed over 6000 security management systems world-wide.

B. *License-Based Expansion.* SMS capacities shall be expandable via software licenses, without the need to load additional software.

2.04 SECURITY MANAGEMENT SYSTEM (SMS) SOFTWARE

A. SMS Software shall be:

1. *Modular:* providing a suite of software modules and options that may be combined to create a seamless integrated security management system platform.

2. *Scalable:* suitable small/medium facilities up to large multi-building and multi-site security management system applications

3. *Intuitive:* use is self-evident; does not require use of reason, experimentation, assistance, or special training.

4. *Arrangeable:* fully configurable select menus and tabs; application workspaces and task windows are configurable as to size and location on the desktop and can be floating; allowing them to be moved around the desktop or across multiple monitors.

5. *Task-oriented:* including the following workspaces:

a. Alarm Event Reporting.

b. Transaction Event Reporting.
c. Graphical Maps.
d. System Status.
e. Cardholder Photo Display.
f. Alarm Notes/Comments.
g. Video Display.

6. *OS-Compatible:* 64-bit native application run on 64-bit versions the following operating systems:

   a. Windows 10 (x64)
   b. Windows 11 (x64)
   c. Windows Server 2022 (x64)
   d. Windows Server 2019 (x64)
   e. Windows Server 2016 (x64)

7. *Database-Compatible:* ODBC compliant and fully compatible with the following SQL database engines:

   a. SQL Server 2019
   b. SQL Server 2017
   c. SQL Server 2016 XP1

8. *Standards-based:* supporting standard Ethernet network communications, industry standard field controller hardware, and other standard-based systems and devices.

9. *Integratable:* easily integrates / interfaces with 3rd-party software and hardware using standards-based protocols and available SDK's and/or API's.

10. *Client-Server-Based:* utilizing a true client-server architecture.

11. *Multi-User:* true multi-user, multi-tasking operation, whereby all system administration and command & control functionality shall be available at any workstation – subject to user authentication and individually defined operator permissions & restrictions.

12. *Browser-based:* Password controlled Accessibility using a standard Internet Browser, providing administration and Command/Control functions.

13. *Auditable:* creating and maintaining an event/transaction log file on the server hard drive; containing all alarm events, card access control transactions, operator actions, and any other event processed and/or reported by the system; with utilities to review log records and create historical data reports in a variety of formats.

14. *On-Line HELP:* providing context sensitive help information text that can be requested with a single keystroke, click of the mouse, or by manual selection at any time - displaying information specific to the configuration or monitoring function that the operator is currently working with.

15. *Multi-Language:* with a user-definable default system language, and operator-specific language selection, supporting following language choices:
    a. English.
    b. Spanish.
    c. Arabic.
    d. Croatian.
    e. Danish.
    f. Dutch.
    g. French.
    h. German.
    i. Greek.
    j. Hebrew.
    k. Italian.
    l. Polish.
    m. Portuguese.
    n. Russian.
    o. Serbian.
    p. Turkish.
    q. Ukrainian.
16. *Data-Secure:* utilizing AES 128-bit and 256-bit Data Encryption to protect data communications between the host server and client workstations, between host server and area controller hardware, and between area controller hardware and local door controller hardware.
17. *High Availability:* supporting fully redundant dual file servers in a hot-standby configuration, using optional application software; upon failure of primary file server, the system shall automatically switch control to the secondary file server with no operator intervention.
18. *Expandable:* with a base SMS configuration including a File Server and supporting a minimum of five Client Workstations, and optionally expandable to support an unlimited number of:
    a. Client Workstations.
    b. Area Controllers.
    c. Door Controllers.
    d. Card Readers.
    e. Cardholder Records.
    f. Inputs.
    g. Outputs.
    h. Access Levels.
    i. Video Sources.
19. *Network-Centric:* with communication via TCP/IP network from Server to Client Workstations, field level Area and Door Controllers, Video System components, and external compatible systems.
20. *Virtualizable:* supporting operation in a virtualized environment via Microsoft Virtual Server or Microsoft Virtual PC guest PCs.

2.05 ACCESS CONTROL SOFTWARE MODULE

A. Cardholder Records

1. Cardholder records shall be configurable through the addition of user-defined fields, and the definition of various data entry templates based on personnel classifications and/or data classifications.
2. Each cardholder record shall support the assignment of multiple cards/credentials and multiple access levels with access schedules.
3. Access shall be assignable to any cardholder and card on a per-door basis as well as via access levels.

B. Capacities

1. *Cardholders:* unlimited number of cardholder records in the access control system database.
2. *Card Readers:* minimum of 32 card readers, expandable to an unlimited number of card readers.
3. *Card Data Formats:* up to eight (8) different access control card formats, configurable and assignable as part of the card reader/door configuration, to allow for different card and card reader technologies to be installed within the same system.
4. *Alarm Inputs:* minimum of 128 alarm inputs, and shall be expandable to support an unlimited number of Alarm Inputs.
5. *Relay Outputs:* minimum of 128 relay outputs, expandable to support an unlimited number of relay outputs.
6. *Controllers:* unlimited number of field level area controllers, local door controllers, and input/output controllers.
7. *Access Levels:* unlimited number of access levels. Access levels shall provide the definition of what doors a cardholder is authorized to access according to specified schedules. SMS software shall support the assignment of multiple access levels to a single cardholder.
8. *Schedules:* creation and configuration of an unlimited number of schedules; each schedule having specific day and time criteria applicable to various hardware & software time-controlled functions within the system, including cardholder access privileges at doors and scheduled override commands to system devices.

C. Distributed Data Processing Architecture

1. SMS shall have a distributed data and processing architecture under which:
   a. *Software to Controller Communication:* the Access control software communicates with area controllers, door controllers, and input and output hardware, to download cardholder database and system

operational parameters, and to perform control actions such manual door unlock commands.

b. *Autonomous Access Request Processing:* Area controllers process cardholder access requests at card readers with no assistance from the server.

c. *Real Time Event Information:* Area controllers transmit system event information to the access control software in real time.

d. *Logging and Reporting:* SMS access control software monitors, reports, and logs all access control system activity in real time.

1) *Ordinary Transactions:* Card reader/keypad transactions shall be received by the system server as they occur in real time, and shall be reported to the operator in the system transaction log display, and permanently recorded/logged in the system activity log file.

2) *Alarm Transactions:* Improper activity and door alarm condition transactions, such as ‘door forced open’ without a card request, ‘door held open’ too long after a valid access transaction or request to exit, card reader tamper condition, and all invalid access requests, shall also be reported to the operator in the system transaction log display, and permanently recorded/logged in the system activity log file.

D. System Configuration

1. *Configuration Utilities:* SMS access control software shall include configuration utilities, as part of the user interface, for each system component and function to allow the customization of the overall system functionality to meet the requirements of the user.

E. Alarm Monitoring and Control

1. *Alarm and Event Monitoring.* SMS access control software shall provide full-feature alarm monitoring and control of alarm, trouble, and off-normal conditions from various devices, including card reader controlled doors and any other type of alarm sensor connected to inputs on the system.

2. *Real Time Alarm Functions.* SMS access control software desktop display shall provide system monitoring and control functions, including an alarm log window, a transaction log window, interactive graphical plans, system status window, and other supporting functions.

3. *Operator Alarm Response Actions.* An alarm log window shall display alarm events, including alarm events that require an acknowledgement and other action by the operator, and alarm event instructions, sorted in by date/time order and by assigned priority.

4. Input Alarm Zones

a. *Alarm Zone Function:* SMS access control software shall support the creation of input alarms zones that allow for enabling or disabling input events.

b. *Alarm Zone Name:* Each alarm zone shall have a user-assignable name of up to 80 characters.

c. *Alarm Zone Control:* Alarm zones shall be able to be scheduled, and manually controlled via the system or via input / output control.

d. *Alarm Zone Status Display:* SMS access control software shall:

1) Present the status of all an alarm zone's inputs before the alarm zone is set.

2) Display disabled input points in the system status window.

e. *Alarm Zone Status Relay:* Each alarm zone shall be linkable to an output so that the output's state will reflect alarm zone's status.

5. Event / Input / Output Linked Actions

a. *Linkable System Actions.* SMS shall provide event or input linking to system actions including output control. Any of the following system actions shall be linkable to an event or input change of state:

1) Door Momentary Unlock.
2) Door Unlock.
3) Door Lock.
4) Door Group Momentary Unlock.
5) Door Group Unlock.
6) Door Group Lock.
7) Door Lockdown.
8) Door Lockdown Clear.
9) Output Momentary On.
10) Output On.
11) Output Off.
12) Sensor Shunt.
13) Sensor Enable.
14) Alarm Zone Arm.
15) Alarm Zone Disarm.
16) Alarm Zone Toggle.
17) Execute Program.
18) Execute SQL.
19) Report Print.
20) Report Display.
21) Send Email.
22) Import / Export.
23) Monitor View Select.
24) Monitor Alarm Start.
25) Monitor Alarm End.
26) Monitor Go Preset.

b. *Link Action Scheduled Control.* The linked actions shall be schedulable so that they can occur only within specified time periods.

c. *Input Link Disabling.* Linked actions shall be configurable to execute or not execute if a designated input is disabled.

6. System Event Instruction Text

a. *Custom Instructions.* SMS shall provide for editing of operator instruction text that is assigned to each system Alarm and/or Event Message either on a global basis or independently for each individual input. The instruction text will be displayed in the Alarm Log Window whenever that assigned Alarm or Event Message is reported

b. *Instruction Size.* Event Instruction text may be up to 100 Characters.

7. System Event Messages

a. *Custom System Messages:* SMS shall provide the option to edit system event messages as a global setting or on an individual input point basis.

8. System Event Sounds

a. *Custom Event Sounds.* SMS shall support assignable sound files to system event messages as either a global setting or on a per-input basis. The default assignable sound files shall be standard .WAV files. The sound files would be activated when that particular event message is reported in the Alarm Log Window.

b. *Sound File Format.* SMS shall support .WAV sound files and allow system administrators to add sound files that can be selected for assignment to events.

c. *Windows Sound Recorder:* SMS custom sound feature shall also support voice annunciation of alarm message information through the use of an internal voice enunciation module. The voice annunciation is configurable as to what portion of the event message are annunciated by voice.

9. System Alarm Configuration

a. *Configurable Alarm Display.* SMS shall allow the display of system alarms to be configurable as follows:

1) *Alarm Display Destinations.* Display at one or more SMS workstations.

2) *Alarm Priorities.* Alarms shall have priorities by which higher-priority alarms are placed above lower-priority alarms in the alarm window.

3) *Alarm Message Consolidation.* The alarm information display shall optionally include the number of times a particular alarm has occurred prior to being acknowledged or cleared, replacing

multiple alarm messages with a single message including the alarm count.

4) *Alarm Window Priority.* SMS alarm window shall be displayed as the topmost window, in front of any other open program windows, as long as there is at least one active alarm.

5) *Alarm Configuration Options:* SMS alarm events shall be configurable so that:

a) An operator must type or assign commentary/notes to the alarm message report before the alarm can be acknowledged.

b) The alarm message can be set so that it cannot be acknowledged if the alarm point is still in an alarm state.

c) Alarm messages can be printed.

d) Alarm messages can be set to have a voice or sound assigned to them.

e) Alarms can display a predefined Instruction text for the system operators.

f) Interactive plans will display the assigned floorplan and Icon.

g) Alarm acknowledgement can be applied to individual alarms or to all alarms at once.

h) All video images associated with the alarm or alarm point can be automatically displayed within the video window.

i) Video cameras can automatically go to any pre-programmed preset.

10. Color Coding for Alarm / Message Priorities

a. *Assignable Alarm Colors.* The colors of any reported alarm/event message shall be assignable based on the alarm / message priorities. Colors shall be selectable from a basic list of colors or via a palette with a wider range of colors.

11. Alarm Notes

a. *Alarm Response Notes.* SMS shall support pre-defined alarm notes (responses) assignable to individual alarms. SMS shall provide system administrators the capability to define additional alarm notes.

12. Transaction Monitoring Window.

a. *Configurable Data Display.* SMS shall allow System Administrators and System Operators to define which of the following data columns are displayed in the Main Transaction Monitoring Window.

1) Location.
1) Event.

2) Details.
3) Badge Number.
4) Department.

13. Manual Control

a. *Operator Manual Control.* SMS shall provide the system operator the option to manually control system components. The manual control interface should include the ability to:

1) Unlock doors.
2) Lock doors.
3) Momentarily unlock doors.
4) Lockdown doors (reader disabled).
5) Lockdown clear.
6) Activate output relays.
7) Deactivate output relays.
8) Arm alarm zones.
9) Force arm alarm zones.
10) Disarm alarm zones.
11) Provide status of connected sensors.
12) Initialize hardware panels.
13) Send individual commands to hardware panels.
14) Move all cardholders within anti-passback areas.
15) Move individual cardholders within anti-passback areas.
16) Send individual commands to integrated devices.

14. Interactive Graphical Plans

a. *Floor Plans and Maps:* SMS shall support the use of interactive graphical plans and maps. Configuration of plans shall allow for the linking of maps via navigation Icons, allowing SMS user to navigate between maps with single mouse click. There shall be no limit to the number of plans or maps that can be used in SMS. The assignable interactive icons shall be:

1) Door Readers.
2) Door Groups.
3) Inputs (sensors).
4) Alarm Zones.
5) Outputs.
6) Outputs Groups.
7) Command Buttons.
8) Field Hardware.

b. *Graphic Formats:* SMS shall support the following graphic formats for maps and plans:

1) JPEG (.jpg).
2) Windows Metafile (.wmf, .emf).
3) Windows Bitmap (.bmp, .dib).

c. *Icon Commands:* SMS interactive plans shall allow system operators to interact with the Icons to perform commands, such as: Lock, Unlock, Momentary Unlock, Lockdown and Lockdown Clear for a door, or acknowledge alarms, etc.

d. *Plan Configuration:* SMS Plans shall be configurable as follows:

1) Plans window location on SMS desktop.

2) Whether or not the Plans window shall be docked or movable.

3) Specify a Plan as the default plan.

4) Specify a time period that a plan will remain displayed after its alarm condition is acknowledged and before returning to the default plan.

5) Whether plans should automatically 'jump' to the specific plan display on alarm, or wait for the operator to manually select the plan which has the active alarm.

6) Icon size.

7) Icon blink rate when in alarm condition.

8) Optionally display the name and status of a point on a plan if the cursor is placed over the point's icon (fly over).

e. Interactive Plan Icons

1) SMS shall contain over 100 predefined Icon's for use on the interactive plans.

2) SMS shall allow for new icons to be uploaded into the database and be available within SMS.

f. Interactive Plan Command Buttons

1) SMS shall support adding specific command buttons to the interactive plan, to enable operators to perform specific commands, such as:

a) Print a selected Report.
b) Display a selected Report.
c) Execute a third-party program.
d) Execute an SQL.
e) Change video surveillance image Views.

F. Area Controller and Door Controller Configuration

1. *Ethernet Communication.* SMS software shall communicate with intelligent area controllers via standard TCP/IP Ethernet protocols.

2. *Card Types Supported.* SMS software shall support the configuration requirements for multiple card technologies, including 125Khz proximity, 13.56Mhz smart card technologies (iClass, Mifare, etc.), Wiegand, OSDP, OSDP SC, magnetic stripe, keypads, biometric devices, bar code, and

wireless lock sets. Data interface to the card readers shall support standard Wiegand Data1 / Data0, OSDP, OSDP SC, as well as Clock/Data protocols.

3. *Fully Configurable.* All operational parameters for the area controllers, door controllers and the specific card readers shall be completely user-configurable via SMS software.

G. Network Device Monitor Application

1. *Network Component Status.* SMS Network Device Monitor Application shall monitor and report status of the network components of SMS system, as well as other devices connected on the network with an IP address, including routers, managed switches, Video System Servers, Internet/Intranet sites, etc. The network device monitor acts as a dashboard running as a Windows Service and functions independently of the SMS software. This enables the desktop dashboard to display the operational status of the monitored network components in the System Status window.

2. *Application Installation.* The Network Device Monitor Application shall normally be installed on the SQL Server Database machine as all it requires is the database to be online.

3. *Monitoring Scope.* When installed, it shall automatically monitor the status of Area Controller Panels of SMS System. The User can then add the definitions of other network devices to be monitored, based on their IP Address.

4. *Online / Offline Device Status.* The System Status Window of the Desktop shall include a selection for “System Monitor”, which will display the online / offline operational status, in real time, of all the designated network devices that are connected to SMS, based on regular communication checks to these devices.

5. *Communications Monitoring.* SMS shall manage the communications to all devices deployed in the system. Due to the critical nature of managing the communications to / from devices interfaced to SMS, the network device monitor shall monitor and display the real-time status and performance characteristics of all on-line communication with the field controllers and devices. Performance monitoring shall inform and warn the operator of any performance issues and degradations, including:

   a. The quality of communication and percentage of connected devices that are on-line.

   b. The average number of polls sent & received from the Communication Manager to field controllers per second.

   c. The average time, in milliseconds, to poll each field controller.

   d. The average time, in milliseconds, to process a received event message.

   e. The event frequency, showing the number of event messages received per second.

f. The latency, or time delay in seconds, for processing received event messages.

g. The number of events in the database queue waiting to be processed.

h. The number of processed events in the process queue waiting to be sent to the Client Desktop(s) to be annunciated and displayed.

6. *Device Tree Display.* SMS network device monitor shall display a graphical device tree showing the live status of all devices connected to SMS. The network device monitor shall also display a running and time stamped stream of communication between the network device manager and the devices connected to SMS.

H. Access Control Functionality

1. FIPS-201 Support

a. SMS shall support the use of FIPS-201 compliant card readers and cards/badges (such as Government issued CAC and PIV cards). The cardholder management screen will allow for programming of the following fields for the credential.

1) Agency.
2) System.
3) Credential or Unique ID.

2. Card Reader Configuration

a. Card reader/door configuration shall include the following user-definable parameters

1) Alarm Shunt Output.
2) Hard Anti-passback.
3) Soft Anti-passback.
4) Area Entering.
5) Area Exiting.
6) Assign Door Lock Output.
7) Assign REX Input.
8) Assign Door Sensor Input.
9) Badge Format mask.
10) Card Data Format.
11) Delayed Access Messages (reporting access transaction only after the door has been opened).
12) Double Card Read Function.
13) Elevator Reader.
14) Failsafe Lock.
15) Failsafe Site Code Verification.
16) Failsafe unlock.
17) Door Held Open Delay Time.
18) Extended Door Help Open Delay Time (for ADA operation).
19) Keypad Mode (keypad/PIN only, card & keypad/PIN, card or keypad/PIN).

20) Led Drive Mode.
21) Lock Door on Close.
22) Lock Door on Open.
23) Log access transaction when door is unlocked.
24) One Door Paired Reader.
25) Rex Bypass (do not activate door lock on REX).
26) Schedule Door Unlock.
27) Schedule Keypad Only Entry.
28) Schedule Reader and Keypad Entry.
29) Schedule Reader or Keypad Entry.
30) Time and Attendance Logging.
31) Two Badge Operation.
32) Unlock Time.
33) Extended Unlock (for ADA operation).
34) Maximum Usage Count.

3. Two Badge Operation

   a. SMS shall support two-badge operation on a per-reader basis, under which two different valid badges must be presented within 15 seconds to unlock a door.

      1) If the second badge presentation does not occur within 15 seconds of the first badge presentation; the first badge presentation shall be disregarded and two different valid badges presentations must be performed.

4. Schedules and Scheduled commands

   a. SMS shall support creating and storing an unlimited number of schedules for use in the System.

      1) *Schedule Names.* Each schedule shall have assignable alphanumeric name of up to 40 characters.

      2) *Schedule Time Intervals.* A schedule shall be defined as specific time interval (start & stop time) on specific days of the week. Multiple time intervals can be applied to the same day of the week. Up to twelve (12) different time intervals may be defined within the same schedule.

      3) *Holidays.* SMS shall support the definition of an unlimited number of holidays or special days, including the definition of eight different types of holidays/special days.

      4) *Schedule Usage.* Schedules shall be assignable for the following functions:

         a) Automatic Card Reader Control & Functionality.
         b) Access Levels.
         c) Precision Access Levels.
         d) Automatic Commands to Alarm Sensors.
         e) Automatic Commands to Alarm Zones.

f) Automatic Commands to Relay Outputs.
g) Scheduled control of Event / Input / Output Links & Actions.
h) Automatic Reports.
i) Scheduled Reminder Reports.

b. One-Time Events

1) One-time events shall be definable within a schedule.

2) Each one-time event shall have a start and end date and a start and end time.

3) One-time events shall be stored in area controllers so that one-time event functionality can be maintained in the event a controller is offline from the SMS or vice versa.

5. Scheduling of System Functions

a. *Schedulable Functions.* SMS shall provide schedulable system functions. A scheduling utility shall allow system administrators to schedule system actions to occur on a one-time or recurring basis. Recurring schedules shall be configured to begin immediately, last indefinitely, or have optional start and end dates.

1) Actions that shall be schedulable include but are not limited to:

a) Event Archiving / Purging.
b) Arm / Disarm Area.
c) Start of Guard Tour.
d) Import of external data via import module.
e) Activate, Deactivate, and Pulse a Device Output and Device Output Groups.
f) Global Anti-Passback Reset.
g) Download Database to AC's.
h) Mask / Unmask Sensor events, Door Forced Open or Held Open.
i) Open Door, Open Door Group.
j) Automatic Reports.
k) Deactivate Badges.
l) SQL scripts for direct interaction with the database.

6. Anti-Passback

a. *Global Antipassback.* SMS shall have the ability for card readers to be configured for anti-passback functionality. SMS shall allow for hard anti-passback, soft anti-passback and timed anti-passback, on a per-card-reader basis. The anti-passback function shall not be limited to readers connected to the same area controller, or readers connected to the same SMS communication server. A true global anti-passback system must be provided.

1) SMS shall allow the designation of an unlimited number of areas, with card readers assigned to specific areas for anti-passback control.

2) Each area shall have an assignable alphanumeric name of up to 40 characters.

3) The System shall allow the card reader configuration of the following anti-passback functions:

a) Hard anti-passback.
b) Soft anti-passback.
c) Timed anti-passback.
d) Are Entry Reader.
e) Area Exit Reader.

b. *Definitions.* See B. 2. Antipassback on page 3 for the definitions of Hard, Soft and Timed anti-passback.

7. Double Card Read Functionality

a. The SMS shall include configurable functionality based on the occurrence of a Double Card Read at specific Card Readers. This function requires two (2) Reads of the Same Card within five (5) seconds at the same Reader. This action will result in the configurable triggering of actions, such as:

1) Toggling the Lock/Unlock status of the same Card Reader door, or a different Door.
2) Execute a Lockdown command to a specific Door.
3) Change the operational mode of the Card Reader.
4) And other configurable commands.

8. Clean Room Functionality

a. *Decontamination Process Enforcement.* SMS shall include clean room functionality for controlling the flow of access to and egress from sensitive areas that have a risk of material cross contamination. Once a cardholder is granted access into a clean room decontamination area, that cardholder will then be granted further access into one lab area only. Upon exiting the lab, users will not be permitted access to any other lab area until they have once again passed through the clean room decontamination area. This functionality helps assure that cardholders may not pass between controlled areas (labs) without first having competed the clean room decontamination process.

9. Red Card/Green Card Functionality

a. *Card-Based Area Control.* Red Card/Green Card functionality allows for designated pairs of cards to be programmed to modify the operational state of a Door when the Red Card/Green Card is presented at designated card readers. Upon reading a Red Card/Green Card, the state of area control shall be modified according to the user defined

attributes for that specific card. The Red Card/Green Card function may also be used, for example, to lock down all doors (or a specified group of doors), or unlock all doors (or a specified group of doors) as a result of defined events.

10. Calendars

    a. *Time Zone Support.* SMS shall support multiple calendars for use in SMS. Calendars can be applied to individual area controllers to account for time zone and other calendar geography-related differences that impact the operation of regional and global security systems.

        1) Calendars shall support the use of eight (8) different types of special days (Holidays).

        2) SMS shall allow for the use of multiple calendars within the same system to provide for system operation across multiple time zones.

    b. *Common Calendars.* Supported calendar formats shall include:

        1) Gregorian calendar.
        2) Hijri calendar (a lunar calendar).

I. Operator Access and Permissions

1. *Administrators and General Operators.* SMS shall support the definition of unlimited number of system operators. Operators shall be defined as either administrators or general operators. Administrators shall automatically have access permission to all functions of SMS software.

2. *Logon Credentials.* Each system operator shall have assignable a unique operator name and password. The operator password shall consist of up to 16 alphanumeric characters.

3. *Operator Access Schedules.* A schedule shall be assigned to each operator to further define the times and days that each operator can have access to SMS.

4. *Discrete Permissions.* Each system operator shall be definable with specific access permissions on a per menu or function basis within SMS software. Operator permissions can be specified as full permission, read-only, or no permission for each of the specific configuration, monitoring, and command functions, as well as specific reports within report generation.

5. *Permission Expiration.* Defined operators shall have the option for an expiration date, causing that operator to be restricted from SMS access upon expiration.

6. *Database Partitions.* SMS shall support database partitions. Partitions shall be defined as segments of the System database, and operators can be assigned to specific partitions allowing them to interact only with the data of that partition. Database partitions shall include:

    a. Cardholders.

b. Access Levels.
c. Card Readers (Doors).
d. Alarm Inputs.
e. Alarm Outputs.
f. Alarm Output Groups.

J. *Operator Language Designation.* Operator definitions shall also include a designated system language for that operator. When the operator logs onto SMS, the chosen language shall be used throughout SMS screens and menus. The operator's language setting can be different than the default language setting for the desktop.

K. Cardholder Credential Management

1. *Credential Management Utility.* SMS shall include a cardholder credential management utility. The utility shall support the creation and maintenance of cardholder records. SMS shall have system operator permission levels for full access, or read-only access, to the cardholder Utility.

2. *Customizable Cardholder Data Records.* Cardholder data records shall be customizable through the creation of user-defined fields. An unlimited number of user-defined fields shall be supported. User-defined fields shall be configurable with specific field names, data field length (# of characters), specific data type, and other parameters.

3. Cardholder Categories

a. SMS shall support categories of cardholders, including employees, contractors, visitors, and others.

b. SMS shall provide user-definable cardholder categories, with no limit on the number of cardholder categories that can be defined.

c. SMS shall allow different sets of data fields to be used for different categories of cardholder records.

d. Key Cardholder Record Fields

1) *Card Number.* The cardholder record shall support a card/badge number of up to 19 digits. The card/badge # can be entered manually, or read into the record via an enrollment card reader. Multiple cards/badges can be assigned to a single cardholder.

2) *Cardholder PIN.* The cardholder record shall support the assignment of a PIN. The PIN shall be used at keypad equipped card readers, and can be entered in conjunction with the card when requesting access at a door. The system shall support a PIN of up to eight (8) digits.

3) *Activation and Expiration.* Each cardholder record shall have an activation date and a deactivation date assigned to the cardholder. Default dates can be configured to be assigned to new card records.

4) *Biometrics.* The cardholder/credential management utility shall support a fully integrated biometric fingerprint enrollment function. This function shall support the enrollment and capturing of the cardholder's fingerprint template(s) directly within the cardholder management application. There shall be no requirement to use an external, 3rd-party software application for the fingerprint enrollment function.

4. Access Levels

   a. SMS shall support the use of access levels for defining what doors/portals a cardholder is authorized to enter. Each access level shall be defined as a list of card reader controlled doors/portals, along with an assigned schedule to designate when the cardholder is authorized to access the doors.

      1) Access levels shall have a user-defined alphanumeric text name of up to 40 characters for easy recognition.

      2) Access levels may be permanent, or temporary if an expiration date is assigned.

      3) Multiple access levels shall be assignable to the same cardholder.

5. *Extended Door Unlock Times for ADA compliance.* The SMS shall support the designation of an extended door unlock time for each cardholder, to enable conformance to ADA requirements. This is a door controller parameter in addition to the extended door unlock time and extended door open time door controller parameters.

6. Card and Cardholder Status

   a. SMS shall provide the designation of a cardholder status, as well as an individual card/badge status. Each status is a means to immediately deactivate a cardholder's access without deleting the cardholder's data record.

      1) Card status and cardholder status are set to "allowed" to be functional at card reader doors. To disable a card, the card status can be set to "expired", "lost", "stolen", "not allowed", or other deactivated status settings. Setting the cardholder status to "not allowed" will disable access for all cards assigned to the cardholder.

      2) SMS shall allow the user to define additional status settings.

7. *Card Trace Mode.* SMS shall provide a "trace" mode for tracking card usage. When a card is set to trace mode, all access control transactions by the card are logged, and reported to the system operator in the alarm log window, highlighted with special text.

8. Bulk Add of Cards/Badges

   a. SMS shall provide a utility to bulk add a range of cards/badge numbers.

1) The bulk add utility shall allow the following data to be set when the cards/badges are added to the system:

a) Starting Badge Number.
b) Quantity of Badges.
c) Last name.
d) Access Level.
e) Precision Template.
f) Card Status.
g) Start Date.
h) Start Time.
i) Expiration Date.
j) Expiration Time.
k) Update Panels.

2.06 REPORT GENERATION SOFTWARE MODULE

A. SMS shall include a full featured Report Generation Utility to display or print database information Reports.

1. The Report Utility shall contain a report wizard allowing operators to create reports tailored for their site. The wizard shall allow the selection of a database table or View, Fields within the table or View, Sort Conditions and a Sort Order.

2. The Report Utility shall contain the following functionality:

a. Over 175 canned (pre-defined) reports.
b. Parameter selection functions.
c. Search between two date/time stamps.
d. Search on event time.
e. Export to text file (TXT).
f. Export to Web Page (HTM).
g. Export to Comma Delimited file (CSV).
h. Export to SQL File (SQL).
i. Email to Recipient.
j. Refresh Time.

3. Table of Canned Reports – The SMS includes over 175 Pre-Defined Reports that can be requested and executed by the Operator. All of these Reports are also editable to all Users to revise the data included in the Report.

2.07 MX+ BROWSER-BASED THIN CLIENT

A. SMS shall include a Mobile-Friendly Thin-Client MX+ Application Module. The MX+ software module shall be a browser-based application for Cardholder Management, Alarm Monitoring, and Door Control.

B. System Access using MX+ shall completely Password controlled.

C. The MX+ Web Server shall require framework 4.7.2 or later.

D. The MX+ Module shall provide administrators the ability to:

1. Add, edit and delete cardholder records.
2. Add, edit and delete access levels.
3. Creation of Schedules
4. Assign and print badges.
5. Assign and display QR Codes on printable badge designs.
6. Monitor and Acknowledge Alarm Events.
7. Control the operation of Reader Controlled doors.
8. Display live Video through the ViewPoint Video Integration Software.
9. Monitor the overall System Status based on status indicators on the Dashboard.

E. Badge templates shall support pictures, QR Code or Bar Codes. Pictures to be applicable from a file or captured using a network-connected webcam.

F. The MX+ Module shall provide the ability to print badges using a network badge printer.

G. The MX+ shall utilize configurable information widgets in a dashboard that graphically informs an administrator about important conditions. Displayable information shall include:

1. Cardholders whose permissions expired today.
2. Cardholders whose permissions will expire in the future.
3. Cardholders added today.
4. Areas last accessed by cardholders.

H. All MX+ Module activity shall be logged for auditing purposes. All event activity that is logged shall include the date, time and name of operator who performed the activity transaction.

2.08 OPTIONAL ***INSITE*** MODULE

A. The SMS shall include the option for the Maxxess InSite Integration, which shall support the capability to administer, manage and support private bi-directional messaging with Mobile Users by means of applications [“apps”] installed on their mobile devices.

B. The InSite integration module provides for combining Systems intelligence and Human Intelligence, in order to dramatically increases users' situational awareness with capabilities to detect and respond to unfolding events in real-time.

C. The situational awareness apps shall be available for mobile devices using common Mobile Operating Systems ["MOSs"] including, at least, Android, iOS, Windows Mobile and BBOS. The apps will be compatible with major mobile carriers including, at least, AT&T, Verizon, T-Mobile and Sprint. The apps shall be comprised of both a native application running under the MOS as well as a \Mobile Web application.

D. All messages within the InSite sub-system shall be logged in a relational database that may be queried by SMS operator to obtain relevant Mobile User or Mobile Group metrics including Mobile User information that is provided consistent with the organization's privacy policy.

E. Messages initiated by Mobile Users will only be sent to SMS and may be classified into two general categories:

1. Duress: messages relating to the Mobile User's personal safety and well-being; and
2. Priority Messaging: messages relating to organizational services and/or action requests unrelated to personal safety.

F. Messages initiated by the system are open in terms of type and content; they may be directed to any set of Mobile Users and may, optionally, include a response Form for Mobile User response. All Mobile User responses will be associated with the initial message from the system. The response form will be structured to allow for effective utilization by the relational database.

G. It shall be possible to utilize the responses of Mobile Users to Forms included with system-initiated messages as valid inputs to the system and/or the EMS. These inputs can initiate appropriate system actions.

2.09 OPTIONAL ELEVATOR CONTROL SOFTWARE MODULE

A. *Elevator Access Control.* SMS shall be capable of optional elevator control, via card readers installed inside an elevator cab, with SMS controlling what floor a cardholder is authorized to access.

B. *Elevator Access Level.* The elevator control shall allow cardholders to be assigned an elevator access level containing floors to be accessible by the cardholder.

C. *Floor Selection Reporting.* SMS shall also provide an option for floor selection reporting, by which the cardholder's floor selection is logged, displayed and reportable by SMS.

D. *Relay Elevator Interface.* SMS shall support elevator control using standard access control hardware, such as standard card readers and standard relay outputs to enable or disable the floor selection buttons inside each elevator cab.

1. *Elevator Floor Selection.* Upon card presentation at the elevator reader by an authorized cardholder, SMS shall active the outputs corresponding to floors

that the cardholder has access to, enabling the cardholder's selection of a destination floor.

E. *Protocol Elevator Interface – OTIS.* SMS shall provide a protocol-based elevator control interface to the OTIS Compass Destination Dispatch system, which includes a destination entry computer (DEC) and a card reader.

1. *User Interaction.* OTIS Destination Dispatch system includes a OTIS destination entry computer (DEC) and a card reader, located in or near the elevator lobby on each building floor. Users interact with the DEC.

a. Cardholders present a card to the reader and select their floor destination using the DEC.

b. Card Reader requests are processed by SMS, which sends a Floor Authorization message to the OTIS Elevator processor.

c. If authorized, the DEC directs the cardholder to the system-selected elevator cab.

F. *Protocol Elevator Interface – SCHINDLER.* SMS shall provide a protocol-based elevator control interface to the SCHINDLER Destination Dispatch system, called its PORT (Personal Occupant Requirement Terminal) Technology.

1. *User Interaction.* SCHINDLER Destination Dispatch system includes a PORT and a card reader, located in or near the elevator lobby on each building floor. Users interact with the PORT.

a. Cardholders present a card to the reader and select their floor destination using the PORT.

b. Card Reader requests are processed by SMS, which sends a Floor Authorization message to the SCHINDLER PORT system.

c. If authorized, the PORT directs the cardholder to the system-selected elevator cab.

2.10 OPTIONAL ID MANAGEMENT & BADGING SOFTWARE MODULE

A. SMS shall support an optional fully integrated ID management and badging utility. An external, stand-alone 3rd-Party ID management and badging system shall not be acceptable.

1. Photo capture shall be performed with an off-the-shelf digital color camera interfaced via a USB Port (or interface card). The software shall provide the functions for on-screen photo capture and storage. Once captured and saved, the photo is stored as part of the cardholder record.

2. Photos can also be imported in a file format (such as .jpg), assigned and stored in the cardholder record.

3. Utilities shall be available for the capture and storage of a cardholder signature. The Signature shall be assigned and stored as part of the cardholder record, and shall be available to be printed on the badge.

4. ID Badge Design
    a. SMS software shall provide utilities for the design and layout of the ID badge format to be printed on the badge.
    b. The Badge design utility shall allow for single or dual sided badge designs.
    c. Data from any data field of the cardholder record, as well imported data images, shall be available to be part of the badge design, including:
        1) Cardholder Photo.
        2) Cardholder Signature.
        3) Imported Artwork, such as a Company Logo or drawing.
        4) Cardholder database fields (text or dates).
        5) Fixed text data.
        6) Card encoding data.
        7) Bar Code fields.
5. Badge design shall allow for different color backgrounds on the badge. It shall also provide the color assignments of text and text background with each field on the badge.
6. Badge Printing
    a. SMS software shall support the printing of cardholder badges, in conjunction with the photo ID and badge design process.
    b. SMS software shall support the interface to an Industry standard dye-sublimation color badge printer.
    c. Badge printers and software shall support single-side or double-side printing, as well as high durability over-laminates, printing of bar codes, internal card data encoders, and other such standard badge printer capabilities.
7. Photo ID Badge Printer
    a. SMS shall support a fully integrated credential management & photo identification badging option. If photo ID badging is required, SMS shall include an ID badge printer. The badge printer shall be a standard dye-sublimation badge printer with a Windows-based driver.
    b. Badge printers shall utilize standard photo quality dye-sublimation / resin thermal transfer technology. Badge printers shall be available in single-side and dual-sided printing capabilities.
    c. ID badge printers shall print edge-to-edge full color ID badges on glossy PVC cards, with lamination. Card lamination may be via the color ribbon or with add-on lamination units.
    d. Various models and options of printers shall be available with printer selection based on the user requirements. Compatible badge printers are:

1) Fargo.
2) Magicard.
3) Zebra.

2.11 OPTIONAL ON-SITE CARDHOLDER TIME & ATTENDANCE REPORTING SOFTWARE MODULE

A. *Time and Attendance.* SMS shall provide an option for cardholder time & attendance calculations, as well as on-site time reporting. This option shall support the designation and configuration of specific card readers for time & attendance purposes.

B. *Time and Attendance Readers.* Card readers shall be designated as “IN” or “OUT” readers. SMS shall provide reporting for total “IN” or on-site time on a per-cardholder basis, with reports showing total time per day or per week. Reports shall be schedulable to run automatically.

C. *3rd-Party Time and Attendance System Interface.* SMS shall allow for time and attendance card readers to store badge reads also in a separate table within the SMS database for query by a third-party time and attendance application.

D. *Muster Reporting.* SMS system shall support on-site mustering reporting. Mustering function shall provide an automatic capability for registering cardholders that are on site during an incident. Designated exit and entry card readers shall be used to enter and exit hazardous locations to/from safe locations. When an incident occurs, a muster report may be generated providing a list of all cardholders that are within the designated muster areas.

2.12 OPTIONAL AUTO IMPORT/EXPORT SOFTWARE MODULE

A. SMS shall provide an optional data import/export utility that allows users to automatically import data fields from a standard comma delimited file extracted from other databases such as Oracle and SQL. The import/export utility shall also allow data to be exported data to delimited files or other external databases.

1. The import/export module shall look for the delimited file then import the data to SMS database.

2. The import/export module shall allow employee data from a human resource database to be imported to SMS database. Changes in the human resource database will be imported into SMS.

3. The import/export module shall allow users to automatically export SMS data to a delimited file.

4. The import/export module shall allow users to scheduling when import/export functions will occur.

B. Database File Import/Export Utility

1. SMS shall include a Utility that will allow the importing of all files into the System SQL Database.

a. The Utility shall allow the following functions:

1) Import / Export of Area Controller Firmware.
2) Import / Export of Icons.
3) Import / Export of Images.
4) Import / Export of Pictures.
5) Import / Export of Sounds.
6) Import / Export of System Templates.
7) Import / Export of Signatures.
8) Import / Export system command files.
9) Import / Export System Status Reports.
10) Rename of files held in database.
11) Allow the files to be set as read only.

2.13 OPTIONAL VIDEO INTEGRATION SOFTWARE MODULE

A. SMS shall provide seamless direct data interfaces to video management systems (VMS). This option shall provide integration with various manufacturer's video controllers, DVRs, NVRs, IP cameras, and video IP servers.

1. This capability will allow for the display, control, recording and archiving of video and text information based on pre-determined events, as well as providing manual command & control directly from SMS interface screen with select devices from the following video system manufacturers:

a. American Dynamics.
b. ACTi
c. ADC DSU1000.
d. Aver (formerly AverMedia).
e. Avigilon Control Center.
f. Axis Video Server and IP Camera.
g. Bosch.
h. Cathexis.
i. Canon.
j. Cieffe.
k. Cisco IP Camera.
l. Crest Electronics.
m. Dedicated Micros.
n. DVTel.
o. Excaq.
p. Geovision.
q. Genetec.
r. Geutebrueck.
s. HikVision.
t. IDIS
u. Infinova
v. Intergral DVX.
w. IQinVision.
x. March Networks.
y. Milestone.
z. Mobotix.
aa. OnSSI.
bb. OpenEye.
cc. Panasonic.
dd. Pelco.
ee. Salient Systems.
ff. Samsung.
gg. Sony IP Camera.
hh. Syac.
ii. Toshiba.
jj. Verint.
kk. Vicon.
ll. Video Insight.
mm. Video IQ.
nn. WebView.
oo. Win4Net

B. SMS shall allow for direct integration to video system DVR's / NVR's, with the following functionality (dependent on the third-party video product's capability include in the SDK):

1. View Live Images.
2. Recorded Image playback.

3. Transaction Search.
4. SMS event Search.
5. Full PTZ Control.
6. Manual Recording Start / Stop.
7. JPEG Snapshot of Live image.
8. JPEG Snapshot of Recorded Image.
9. Download of Video Clip to AVI.
10. Recording start / stop from SMS Event.
11. Send PTZ Presets based on alarm event.
12. Reporting of DVR/NVR/IP CAMERAS Alarm Input events.
13. Reporting of DVR/NVR/IP CAMERAS Analytic alarm events.
14. Instant Replay of last minute.
15. Loss of Connection reporting.
16. Auto Reconnect.

C. SMS Video application must be an open application and allow for any third-party product to be integrated, depending on the third party's capabilities.

1. SMS Video application shall require the minimum of information to connect to the DVR/NVR/IP CAMERAS as below and the application shall auto configure itself. The application should create the camera list detailing whether the camera is a PTZ, has microphone attached or has audio available.

    a. DVR/NVR/IP CAMERA'S Name.
    b. Device Model.
    c. IP Address.
    d. User Name.
    e. Password.

2. SMS Video application shall allow System Administrators to configure the following:

    a. Definition of a specific view, which is the display of multiple cameras from various sources within SMS with a single command.

    b. System Administrators' and system operators' privileges as to which views and cameras they are authorized to display.

    c. Assigning specific cameras or views to a system point, Door reader, input or field hardware.

    d. SMS video application must be able to display web pages alongside video Images.

    e. SMS video application must be fully integrated into SMS. The Video application must be able to react to SMS events and alter views of video images as well as call PTZ presets.

    f. SMS video application shall enable system administrators to create a dynamic view. The dynamic view will automatically activate and display the applicable camera images when the DVR's / NVR's Video Analytics reports an Analytic event. The video application shall allow the system

administrators to control how long the video images are displayed to the operator.

g. Any SMS reported event or transaction that has been assigned a video camera shall then display a small camera Icon on that transaction line. SMS operators can then click on the Icon and the video application will show the recorded images from the camera with the event / alarm time stamp.

h. The video application shall allow the system administrators to control the following:

1) Force the application to start Maximized.
2) Allow / disallow the operator to resize the application.
3) Auto logout of SMS will also logout of video surveillance application.
4) PTZ Joystick control.
5) Enable the video surveillance application to also remain on top of other Windows Applications.
6) The folder for storing of JPEG or AVI files.
7) Playback Pre-delay and Post-delay times.
8) Sounds on System Events.
9) Enable / Disable video surveillance application tabs.
10) Video surveillance system Event Colors.

i. SMS video application should be available as a separate product not requiring SMS to operate.

j. SMS video application shall support the following per-screen Video display configurations:

1) 1 Camera.
2) 4 Cameras.
3) 9 Cameras.
4) 16 Cameras.
5) 25 Cameras.
6) 36 Cameras.
7) 49 Cameras.
8) 64 Cameras.
9) 1 + 5 Cameras.
10) 1 + 12 Cameras.

D. Cardholder Picture display against live image

1. SMS shall support interfacing to a video system and displaying a live video image next to a stored cardholder image record. This feature shall be system configurable and allow for multiple screens displayed in the same window.

E. SMS software shall support multiple video monitors on a single client workstation, providing the capability to configure a virtual desktop across multiple monitor screens.

2.14 OPTIONAL DATABASE INTEGRATION SERVICES SOFTWARE MODULE

A. SMS shall support for interactive database integration services. The database integration services module shall support Active Directory integration with external systems and databases, enabling a single point of data entry across multiple systems and databases. The database integration services module shall run in the background to keep critical data synchronized across disparate systems. A change in data from one system shall be automatically affected in all other designated systems.

B. The database integration services module shall enable federation of systems by mapping group membership in Active Directory to user accounts in the respective systems. The Active Directory connector shall keep the systems synchronized with Active Directory, allowing changes to flow between them; combining near real time synchronization of logical and physical access.

C. The database integration services module shall support data exchange with SQL, MySQL, Oracle, or other external system databases.

2.15 OPTIONAL GUARD TOUR SOFTWARE MODULE

A. SMS software shall optionally support guard tour functionality. The guard tour shall allow for any number of card readers to be defined as part of a guard tour.

B. Each guard tour definition shall have a user-defined alphanumeric name of up to 40 characters.

C. The guard tour shall allow individual credentials to be defined as guard tour cards. The time between points as defined on the guard tour shall be set in 10 second intervals.

1. The Guard tour shall allow for the following features on a tour:

    a. Start.
    b. Pause / Restart.
    c. Abort.

2. The guard tour shall generate an alarm to SMS if the running tour detects:

    a. Late Arrival.
    b. Early Arrival.
    c. Out of Sequence.

3. The guard tour shall allow a tour to be performed in reverse.

4. The guard tour shall allow a tour to be scheduled.

5. SMS shall include reports designed for the guard tour, these are to include:

    a. Configuration of tours.
    b. Tours history.

2.16 OPTIONAL ASSET MANAGEMENT SOFTWARE MODULE

A. SMS cardholder database shall include an optional asset management utility. The asset management function shall support defining specific assets into the database with an access control card or tag, and assigning them to a specific cardholder.

B. Upon an access request at a door/portal, the scanned asset tag must be assigned to the cardholder requesting access, or access will be denied.

2.17 OPTIONAL BUILDING CONTROLS INTEGRATION SOFTWARE MODULE

A. SMS shall provide support for an optional integration and/or interface to external Building Management or HVAC Systems. This includes an operational interface to OPC, BacNet, or LonWorks, providing for the SMS to receive-only and report alarms & events from the external Building Management System.

2.18 OPTIONAL VISITOR MANAGEMENT SOFTWARE MODULE

A. *Description.* SMS shall support the optional implementation of a full featured, fully integrated visitor Management System. The visitor Management System shall incorporate a separate visitor Database, and shall also be available as a stand-alone Visitor Management software package. The visitor management system database shall share data records (import/export) with SMS.

B. *Visitor Management.* The visitor management system software shall provide tools to manage Visitors entering and exiting the facility, including the logging of entry and exit times, issuing of temporary paper visitor badges, issuing of temporary access control card (if applicable), and report generation of visitor activity.

C. *Pre-Enrollment.* The visitor management system shall support visitor pre-enrollment capabilities via a web browser interface.

D. *Visitor Badges.* The visitor management system shall include the capability to issue access control cards/badges to authorized Visitors to allow card reader access to specific areas of the site. The issuance of cards/badges shall create a cardholder record in SMS, with access privileges controllable via SMS.

E. *Visitor Information Scanner.* The visitor management system shall support the capture of visitor personal information via a driver’s license scanner, business card scanner, or passport scanner. Visitor information shall also be enrollable manually via the workstation keyboard. A photo capture option shall also be available.

F. *Temporary Visitor Badges.* The visitor management system shall provide the capability to create and print temporary visitor badges using paper badge stock with the applicable badge printer.

G. *Visitor Reporting.* The visitor management system shall include complete report generation utilities for the creation of visitor Reports showing entry time, exit time, cumulative time on site, Person visited, access control card assignment, etc.

2.19 OPTIONAL 3RD PARTY INTEGRATION SOFTWARE MODULE

A. SMS shall provide a generic interface for third party systems.

1. *Functionality.* SMS shall include a generic library that enables SMS to receive events from other third party system via an ASCII text string.

    a. The received events shall be able to:

        1) Display in the event window.
        2) Display in the alarm window.
        3) Interface with the interactive plans window.
        4) Have dependencies activated based on the event.
        5) Disable the interface library.

    b. The Generic Interface shall enable the following to be programmed:

        1) Name of the generic Interface library.
        2) Communication workstation address.
        3) Enable / Disable.
        4) Debug .
        5) Port settings.
        6) Capture data string.
        7) Heartbeat Time.
        8) Heartbeat String.
        9) Number of lines the data is to be received over.
        10) Sync string.
        11) Time line.
        12) Time Format.
        13) Month String.
        14) Event Line.
        15) Event Format.
        16) Default Event.
        17) Details line.
        18) Details Format.
        19) Panel Line.
        20) Panel String.
        21) Panel Format.
        22) Point Line.
        23) Point String.
        24) Point Format.
        25) Add match.

B. *3rd Party Systems.* SMS shall provide optional software utilities for interfacing and/or integrating with external, 3rd-Party systems, such as fire alarm systems, intrusion detection systems, building management systems, and external database systems such as human resources systems and/or student databases.

    1. *Intrusion Interfaces.* SMS shall include the optional capability to seamlessly interface with selected 3rd Party intrusion detection and alarm devices. This function will provide for annunciation of intrusion and other alarm conditions detected by these panels and devices. The system will support an interface from the following intrusion/alarm system products and manufacturers:

a. BOSCH Alarm Panels - Bi-Directional Interface with GV3 & GV4 Series models include D9412GV3, D7412GV3, D7212GV3, D9412GV4, D7412GV4, and D7212GV4.
b. Honeywell Galaxy - Bi-Directional Interface to the DIMENSION or FLEX panels.
c. Honeywell PRO2200.
d. Honeywell PRO3200.
e. Honeywell Ademco Vista.
f. Bosch D6600 receiver.
g. Bosch 7412 and 9412.
h. DMP.
i. Inovonics Wireless Alarm Devices.
j. Cooper Security – Scantronic.
k. Texecom.

2. *Fire Alarm Interfaces.* SMS shall provide seamless interface with select fire alarm monitoring panels and devices in order to provide for secondary annunciation of alarms and trouble conditions detected by these panels. An interface shall be supported from the following fire alarm manufacturers:

a. Aritech.
b. Inim.
c. Kentec.
d. Notifier.
e. Siemens.
f. Gent.
g. Fire Sentry.
h. Firelite.
i. Edwards EST.

3. *3rd Party Access Control System Integration.* SMS shall include the capability for integration with 3rd-Party Access Controllers. And Interface shall be supported for the following Access Control modules:

a. PCSC IQ200.
b. PCSC IQ400.
c. PCSC IQ600.
d. PCSC IQ800.
e. PCSC IQ1000.
f. PCSC 1200.
g. PCSC SIM Modules.
h. PCSC Fault Tolerant Controller.
i. PCSC Single Door Module (SDM).
j. PCSC Dual Door Module (DDM).
k. Honeywell Pro2200.
l. Honeywell Pro3200.
m. SALTO CU42E Controller.
n. SALTO CU4200 Controller.
o. SALTO SVN Control Units (CU50ENSVN, CU5000).

p. SALTO SALLIS On-line Wireless Locking Products
q. Mercury M5 Family of Controllers.
r. Mercury MS Software House Controller replacements

4. Wireless Alarm Systems

a. *Inovonics Receivers.* SMS shall provide seamless integration between SMS software and the Inovonics family of wireless receivers, repeaters, and sensors. The Inovonics products provide for wireless alarm sensors, motion detectors, panic/duress alarm buttons, door contacts, environmental sensors, and other signals wirelessly transmitted and interfaced directly into SMS via applicable Inovonics wireless receivers/repeaters.

b. *Alarm Events.* The Inovonics wireless alarm sensors shall be configured in SMS database, and will report Alarm Events in the same manner as wired alarm sensors.

2.20 MOBILE IDENTIFICATION AND VERIFICATION MODULE (REMOTEPOINT)

A. The mobile identification and verification module shall allow hand-held PDA devices to be interfaced, via wireless Network, with the Security Management System (SMS). The hand-held PDA devices shall enable remote identification and/or verification of cardholders; such as employees, residents, visitors, contractors, etc. The mobile identification and verification software module shall allow designated security staff to check the validity and identity of the cardholder using a card reader equipped hand-held PDA device that is directly linked, via wireless network, into SMS.

1. The mobile identification and verification module shall be password protected; allowing only authorized users to operate the hand-held PDA device.

2. The mobile identification and verification module shall provide ten (10) user definable PDA icons to be used within the device's graphic user interface.

3. The mobile identification and verification module shall be designed to work with contactless smart cards including HID Global's iClass platform and standard MIFARE technology credentials.

4. The data display for the hand-held mobile device shall be a two-page display that is configurable to include the following information:

a. 1st page: Cardholder Information

1) Picture.
2) Name.
3) ID Number.
4) Cardholder Status.
5) Card Expiration Date.
6) Department / Company Name.
7) The User definable text field that can be up to 255 characters.

b. 2nd page: Cardholder additional information

1) User-defined data fields.

2.21 SECURITY MANAGEMENT SYSTEM (SMS) SERVER AND PC HARDWARE

A. SMS File Server

1. SMS file server shall be a standard PC.
2. SMS file server shall meet the following ***minimum*** requirements:
   a. QUAD Core Processor or better.
   b. 32GB minimum ECC SDRAM.
   c. 16XDVD+/-RW 48X CD ROM.
   d. 500GB or greater SATA 7200 rpm hard drive.
   e. Two 100/1000Mb Ethernet ports configurable for single redundant port operation.
   f. 17” Flat LCD Monitor.
   g. 16MB Video Card.
   h. Sound Card and Speakers for Voice Annunciation.
   i. USB keyboard.
   j. USB optical mouse.
   k. Parallel or USB port for Report Printer.

B. SMS Redundant File Server

1. The Maxxess eFusion System shall offer an option for fully REDUNDANT File Servers.
   a. The Redundant File Servers option utilizes two (2) identical Server machines operating in a Hot Standby mode.
   b. The hardware requirements for the Redundant File Servers shall be two 2U Rack Mount Servers capable of supporting Citrix XenServer.
2. System configured should be at minimum:
   a. Intel VT – Enabled Processor (minimum QUAD Core processor, 6 or 8 Core is better)
   b. 32GB RAM Minimum / 128GB RAM Maximum
   c. 600GB Minimum Total Disk Space Storage
   d. 16MB Video Card minimum
   e. Qty Two (2) 1GB or 10GB NIC’s for server link paths
   f. Qty Two (2) 1GB minimum NIC’s for Management Network
   g. Qty One (1) 100Mb NIC’s for Production Network
   h. Enhanced DVD-ROM/CD-RW Combo Drive
   i. Hot-swap Redundant Power Supply Option

j. Database: Microsoft MS SQL Server 2019, 2017, 2016, 2014, or 2012 Standard Edition.
k. Recommended Operating System: One (1) Microsoft Windows Server 2012, 2016, or 2019 Std with 5 Cals 64 Bit (recommend Enterprise Edition if a larger system)

C. SMS Client Workstation

1. SMS shall support multiple client workstations to be used for system monitoring, command & control, and/or database entry and maintenance.

2. System client workstation minimum requirements shall consist of:

a. Dual Core Processor or better.
b. 8GB minimum ECC SDRAM.
c. 16XDVD+/-RW 48X CD ROM.
d. 100GB minimum SATA 7200 rpm hard drive.
e. 100/1000Mb Ethernet port.
f. 17” Flat LCD Monitor.
g. 16 MB Video Card minimum.
h. Sound Card and Speakers for Voice Annunciation.
i. USB keyboard.
j. USB optical mouse.
k. Parallel or USB port for Report Printer.

D. SMS Client Workstation with Video

1. The Maxxess eFusion Security Management System provides for video surveillance system integration. If the video surveillance system integration option is included, SMS Client workstation will be used for displaying live and recorded Video as well as standard system monitoring and card access control activity. If the client will be used for displaying video, the workstation shall be a standard PC.

2. System Client Workstation for displaying Video minimum requirements shall consist of:

a. Dual Core Processor or better
b. 16GB ECC SDRAM.
c. 16XDVD+/-RW 48X CD ROM.
d. 100GB minimum SATA 7200 rpm hard drive.
e. 100/1000 Ethernet port.
f. 17” Flat LCD Monitor (SVGA 1000 x 800 minimum).
g. 64 MB Dual Monitor Video Card.
h. Sound Card and Speakers for Voice Annunciation.
i. USB keyboard.
j. USB optical mouse.
k. Parallel or USB port for Report Printer.

E. SMS Client Workstation with ID Management

1. The Maxxess eFusion Security Management System shall support the option for full function Photo Identification Badging Station capabilities. The Client Workstation used for a Photo ID Badging Station shall be a Standard PC.
2. System Badging Workstation minimum requirements shall consist of:
    a. Dual Core Processor or better.
    b. 16GB ECC SDRAM.
    c. 16XDVD+/-RW 48X CD ROM.
    d. 100GB minimum SATA 7200 rpm hard drive.
    e. 100/1000 Ethernet port.
    f. 17” Flat LCD Monitor.
    g. 64 MB Dual Monitor Video Card.
    h. Sound Card and Speakers for Voice Annunciation.
    i. USB keyboard.
    j. USB optical mouse.
    k. Parallel or USB port for Report Printer.

2.22 SALTO VIRTUAL NETWORK (SVN) INTEGRATION

A. *Direct Integration.* SMS software shall integrate directly with Salto SVN without the need for additional software application(s). The SVN integration allows Salto SVN enabled stand-alone locks, e-cylinders, and padlocks to read, receive and write information via distributed intelligence using the contactless smart card credential.
    1. User-related access information shall be stored in an encrypted format on credentials.
    2. Online wall readers shall be updated and receive information from the credentials at any time or anywhere in the building.
    3. Salto SVN cards and readers shall be programmed and transactions displayed in SMS application in the same manner as wired on-line locks.

B. *How SVN Works.* The SALTO data-on-card technology shall enable users’ credentials to act as a carrier in order to transmit information from the stand-alone locks to the online hotspots and thereby make the information available to the PC.

C. *Fallback to Wireless Mode.* SMS Salto SVN integration shall enable a wired lock solution to fail to data-on-card (SVN) operation while being transparent to the user population.

2.23 WIRELESS LOCK INTEGRATION

A. SMS shall provide seamless integration for integrated wireless locks via the eMAX-EP controller platform without the need for any optional software. Compatible wireless locks shall include:
    1. Integration with Salto Sallis Locks.
        a. SMS shall provide integration to standard Salto Sallis wireless locks via the eMAX EP platform.

b. Each eMAX EP controller shall support up to sixteen (16) Salto Sallis locks.

c. SMS shall communicate to Sallis wireless locks via standard Salto Sallis repeater and nodes connected to the eMAX EP controller via RS-485 connection.

2. Integration with Assa Abloy Aperio Locks

a. SMS shall provide integration to standard Assa Abloy Aperio v.N2 wireless locks via the eMAX EP platform.

b. Each eMAX EP controller shall support up to sixteen (16) Assa Abloy Aperio locks.

c. SMS shall communicate to Aperio wireless locks via standard Assa Abloy Aperio v.N2 wireless transponders connected to eMAX EP controller via RS-485 connection.

3. Integration with Ingersoll Rand/Allegion Locks

a. SMS shall provide integration to standard Schlage/Allegion ADS-300 wireless locksets via the eMAX EP platform.

b. Each eMAX EP controller shall support up to sixteen (16) ADS-300 locks.

c. SMS shall communicate to ADS-300 wireless locks via standard Schlage/Allegion PIB-2TD panel interface modules connected to the eMAX EP controller via RS-485 connection.

END OF SECTION

Formatting	
Font:	Arial 10
Header and Footer:	Arial 9
Margins:	1”, 1”, 1”, 1”
From Edge:	Header 0.5”, Footer 0.4”
Indents:	0.5”, 0.375”, 0.375”, 0.375”, 0.375”, 0.375”
Format:	Specification is based on MasterFormat 2016