SECURITY MANAGEMENT SYSTEM

EcoStruxure Security Expert™ Access and Intrusion System by Schneider Electric

Schneider Electric Editor’s Note:
This guide specification is written in accordance with the Construction Specifications Institute (CSI) Master Format. This section must be carefully reviewed and edited by the architect or the engineer to meet the requirements of the project. Coordinate this section with other specification sections within the Contract Documents and Drawings.
To properly use / edit this document, show formatting and hidden text by selecting ¶ on the menu or by typing (Ctrl+*) simultaneously. Except for these introductory and closing paragraphs, green hidden text will not print. Text in red is optional. Red text in [brackets] denotes multiple options where one or more shall be chosen. All red text shall be edited and changed to black for final project conformation. In addition, these introductory paragraphs shall be deleted or changed to hidden text.
Additional guidance and specifications can be found at https://www.schneider-electric.us/e2e

This specification is typically used for projects needing advanced server-based solutions, functional LED controls, and/or integration to EcoStruxure Building Operation. This specification should be used for projects migrating from an existing Andover Continuum or TAC I/NET Security platform.

PART 1 - GENERAL

1.1 SUMMARY

A. Scope: Provide labor, material, equipment, related services, and supervision required, including, but not limited to, manufacturing, fabrication, configuration and installation for a Security Management System (also identified as SMS, SMS, Access Control System, Intrusion Detection System, Security Control and Monitoring System) as required for the complete performance of the Work, as shown on the Drawings and as specified herein.

B. The SMS shall be provided by a qualified SMS system supplier. The Contractor shall ultimately be responsible for the SMS and shall supplement the system supplier's Work as necessary to provide a complete and operable system. The Contractor shall coordinate the equipment and systems provided by others that interface with the SMS to ensure necessary interconnections and compatibility are provided for the required functionality of the SMS.

C. Related Sections: Related sections include, but shall not be limited to, the following:

1. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

2. Applicable general requirements for Electronic Safety and Security Work specified within Division 28 Specification Sections including those for Common Work Results for Electronic Safety and Security specified within the subset of 28 05 ## specifications apply to this Section. [In addition, refer to the following Division 28 specifications for additional requirements:]
   a. Section 28 46 21 Fire Alarm System

3. Refer to the following specifications for additional requirements related to the integration and interface with the Electrical Power Management System:
   a. Section 23 09 23.11 Direct Digital Control System for HVAC
   b. Section 25 00 10 – Intelligent Building Management System
   c. Section 40 60 10 - Process Instrumentation and Control System
1.2 REFERENCES

A. General, Publications: The publications listed below form a part of this Specification to the extent referenced. The publications are referred to in the text by the basic designation only. The edition/revision of the referenced publications shall be the latest date as of the date of the Contract Documents, unless otherwise specified.

1. Canadian Standards Association (CSA)
   a. CSA C22.1, “Canadian Electrical Code, Part I” (CEC)

2. Federal Communications Commission (FCC)
   a. FCC – Part 15, Part 68, “Connection of Terminal Equipment to Public Switched Telephone Network”

3. National Fire Protection Agency (NFPA)
   a. NFPA 70, “National Electrical Code (NEC)”

4. Underwriters Laboratories (UL)
   a. UL 294, “Standard for Access Control System Units”
   b. UL 1610, “Standard for Central-Station Burglar-Alarm Units”
   c. ULC, “UL Standards for Canada”

1.3 DEFINITIONS

A. Unless specifically defined within the Contract Documents, the words or acronyms contained within this specification shall be as defined within, or by the references listed within this specification, the Contract Documents, or, if not listed by either, by common industry practice.

1. SMS: Security Management System
2. iSMS: Intelligent Security Management System or Integrated Security Management System
3. ACS: Access Control System
4. IDS: Intrusion Detection System

1.4 SUBMITTALS

A. General: Submittals shall be in accordance with the requirements of Section [01 33 00][01300] Submittals, in addition to those specified herein.

1. Submit sufficient information to determine compliance with the Contract Documents. Identify submittal data with the specific equipment tags and/or service descriptions to which they pertain. Submittal data shall be clearly marked to identify the specific model numbers, options, and features of equipment and work proposed.

2. Deviations from the Contract Documents shall be indicated within the submittal. Each deviation shall reference the corresponding drawing or specification number, show the Contract Document requirement text and/or illustration, and shall be accompanied by a detailed written justification for the deviation.

3. Submit required product data and shop drawings specific to each product and accessory proposed. In addition, include the following information:
   a. 

B. Operation & Maintenance (O&M) manuals shall be provided in accordance with the minimum requirements specified in Section [01 78 23][1780] Operation and Maintenance Data and additional requirements specified herein.

1. Documentation relating to the installation, programming and operation of the system shall support the system.
2. Software Documentation: Security software documentation must be provided to ensure the proper installation and maintenance of the system. The range of software documentation shall include:
   a. An installation guide that describes installation procedure and troubleshooting
   b. An operator's guide that details the programming fields within the system
   c. A network administration guide that outlines the operation of the various networking and communication protocols used by the system.
   d. The system shall also include a comprehensive online help system that is available directly through the software.

3. Hardware Documentation: Security hardware documentation must be provided for the relevant modules/devices being installed to ensure proper installation and maintenance. The range of hardware documentation shall include:
   a. An installation guide that includes hardware wiring with the necessary diagrams, configuration, mechanical layouts, technical specifications, ordering information and warranty.
   b. A quick start guide with an overview of hardware wiring and configuration
   c. A UL installation sticker (if the product has been UL certified) that shall have an overview of hardware wiring and configuration.

4. Application Notes: Application notes that cover specific integrations or features shall be available to assist in system programming.

5. API Documentation: Documentation for the Automation and Control Protocol and SOAP Service that outlines the API and instructions for programming third party software to communicate with the system shall also be available.

1.5 QUALITY ASSURANCE

A. Manufacturer Qualifications: Manufacturer shall be a firm engaged in the manufacture of specified products of types and sizes required, and whose products have been in satisfactory use in similar service for a minimum of ten years.
   1. The manufacturer shall have a valid ISO 9001 certification and an applicable quality assurance system that is regularly reviewed and audited by a third-party registrar. Manufacturing, inspection, and testing procedures shall be developed and controlled under the guidelines of the quality assurance system.
   2. The manufacturer or their representative shall have service, repair, and technical support services available 24 hours 7 days a week basis.

B. Installer Qualifications: Installer shall be a firm that shall have a minimum of [10] years of successful installation experience with projects utilizing equipment similar in type and scope to that required for this Project [and shall be approved by the manufacturer's representative].
   1. The system shall only be installed and managed by technicians holding at least a current Security Level 1 certification by the manufacturer of the system being installed. There are currently three levels of certification:
      a. Installer
      b. Integrator
      c. Administrator

C. All work performed, and all materials used shall be in accordance with the [National Electrical Code], [Canadian Electrical Code] and with applicable local regulations and ordinances. Equipment assemblies, materials, and equipment shall be listed and labeled by Underwriter's Laboratories or by a testing agency acceptable to authorities having jurisdiction and marked for intended use.
1.6 DELIVERY, STORAGE AND HANDLING

A. Prior to delivery to the Project site, ensure that suitable storage space is available to store materials in a well-ventilated area protected from weather, moisture, soiling, extreme temperatures, humidity, and corrosive atmospheres. Materials shall be protected during delivery and storage and shall not exceed the manufacturer stated storage requirements. As a minimum, store indoors in clean, dry space with uniform temperature to prevent condensation. In addition, protect electronics from all forms of electrical and magnetic energy that could reasonably cause damage.

B. Deliver materials to the Project site in supplier’s or manufacturer’s original wrappings and containers, labeled with supplier’s or manufacturer’s name, material or product brand name, and equipment tag number or service name as identified within the Contract Documents.

C. Inspect and report any concealed damage or violation of delivery storage, and handling requirements to the Engineer.

1.7 WARRANTY

A. General: Refer to [Section 01 77 00 - Closeout Procedures] [Section 01770 - Closeout Procedures].

B. The manufacturer shall warrant products against defects in material and workmanship for [12 months from the date of commissioning or 18 months from the date of shipment – whichever comes first.] [24 months from the date of commissioning or 36 months from the date of shipment, whichever comes first, provided that the manufacturer performs functional testing, commissioning and first parameter adjusting of equipment.] During the warranty period the manufacturer shall repair or replace defective products. This warranty shall be in addition to any provided by the Contractor. The warranty shall exclude normal wear and tear under normal usage and any damage caused by abuse, modification, or improper maintenance by entities other than the manufacturer or its approved representative.

C. Additional Owner Rights: The warranty shall not deprive the Owner of other rights the Owner may have under other provisions of the Contract Documents and shall be in addition to and run concurrent with other warranties made by the Contractor under requirements of the Contract Documents.

1.8 SPECIAL TOOLS AND SPARE PARTS [- NOT USED]

A. The Contractor shall provide a recommended spare parts list with the following information provided as a minimum:

1. Contact information for the closest parts stocking location to the Owner.
2. Critical spare parts shall be identified as those parts being associated with long lead times and/or those being critical to the unit’s operation.
3. Maintenance spares shall be identified as being those parts required to regularly perform scheduled maintenance on the furnished equipment. These spares shall include, but shall not be limited to, consumable spares that are required to be exchanged during scheduled maintenance periods.

B. Spare parts shall be provided for each type and size of unit installed. At a minimum, the following shall be provided:

1. Provide the minimum spare parts recommended by the manufacturer.
2. Provide [1] set of each type of power and control fuse installed within equipment

C. Any manufacturer specific special tool, not normally found in an electrician’s toolbox, required to remove and install recommended or furnished spare parts shall be furnished. At a minimum the following shall be provided:

1. If available from manufacture[and required to configure equipment], provide PC-based computer configuration software or smart mobile device app tool and a minimum of [one] communication
interface cable for each type of cable required to connect the computer/device to the devices specified herein for configuration and programming.

2. Electronic configuration files, in a media format acceptable by the Owner (e.g. CD, USB stick, etc.), updated to an as-installed and commissioned state.

D. Spare parts shall be properly marked and packaged for long term storage. Printed circuit boards shall be provided in separate anti-static containers.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Basis-of-Design Product: Subject to compliance with requirements, provide EcoStruxure Security Expert by Schneider Electric with supported products and accessories.

B. Acceptable Security Management System Architectures: The architecture of the SMS shall be based on a manufacture of systems who has validated the integration of systems similar in type and scope to that required for this Project. Provide the following specified manufacture’s system architecture without exception, unless allowed as a substitute by addendum to the Contract Documents prior to the bid date:

1. EcoStruxure Security Expert by Schneider Electric
2. [2nd manufacturer and validated architecture]
3. [3rd manufacturer and validated architecture]

C. The Security Management System software, controllers, power supply, expansion modules and card reader technology shall come from one manufacturer. Whenever components are included from sources other than the manufacturer of the system, the Contractor shall demonstrate and verify that the components are compatible, prior to system acceptance, and shall provide to the Owner that use of such components will not void or impair the system warranty.

D. Security Management System specified herein shall be provided by a single system supplier. Systems, products and manufacturers specified are to establish a standard of quality for design, function, materials, and appearance. Products shall be modified as necessary for compliance with requirements. Provide the specified product and manufacturer without exception, unless allowed as a substitute per the general provisions of the Contract.

E. The Contractor shall provide but not be limited to the following major items of equipment required for a complete and operable system.

1. Card Readers / Biometrics Readers / Smart Card Readers / Keypads / Cards
2. Integrated Access Control and Alarm Control Panels
3. Reader / Door Control Unit
4. Zone / Input Alarm Control Unit
5. PGM (Programmable Output) / Alarm Control Output Unit
6. Door Locks Mechanism / Door Lock Power Supplies
7. Safety Disconnection Switch, Fire Alarm Interface and Elevator Control Interface Unit.
8. Central Processing Unit (CPU)
9. Modems, Ethernet Switches and all related communications equipment
10. System Printers
11. Power Supply Devices/Transformers/Backup Batteries
12. Master Desk/Work Station Desk
13. Metal/Steel Equipment Enclosures
14. Client/Workstation Computers
15. Cable/Wire for Card Proximity Readers and Panel Communication
17. Photo Identification Image Capture Camera twain or compatible.
18. Paging System interface and equipment to suit Motorola, POCSAG or suitable RS232 interface device.

2.2 GENERAL REQUIREMENTS

A. Where more than one code or regulation is applicable as listed in Article 1.2 References, the more stringent shall apply unless that code is not applicable in the location of installation.

B. The SMS application shall be a modular, networked security management system capable of handling large corporations with multiple remote sites, access control, intrusion detection, alarm monitoring, video imaging, photo identification, with capabilities to provide integration with 3rd party applications as applicable including but not limited to digital video management systems, building automation system, key management systems, elevator management systems and wireless lock systems. The system shall allow for easy expansion or modification of inputs, outputs, and remote-control stations.

C. Integrated Solution: The system shall support integrated Access Control, Intrusion and IP intercom functions natively. Separate system controllers for Access Control and Intrusion Alarms shall not be acceptable. Separate Security Management Server and VoIP intercom server shall not be acceptable.

D. Security: The system shall be cybersecurity compliant and have standards based, NIST RSA1024 and AES256 bit certified, data encryption throughout the system. All IP communication shall be in accordance with TLS 1.0 standards, TLS 1.2 where applicable.

E. Central Server: The system control at the central computer location shall be under a single server software program control, shall provide full integration of all components, and shall be alterable at any time, depending upon the facility requirements. Reconfiguration shall be accomplished online through system programming, without hardware changes.

F. Operating System: The software program shall be available as a true 32-bit or 64-bit, 3 tier client/server, ODBC compliant application based on Microsoft tools and standards. The program shall operate in one of the following environments:
   1. Microsoft Windows 10 Professional, Enterprise
   2. Microsoft Windows 8.1 All Editions
   3. Microsoft Windows 7 Professional
   4. Microsoft Windows Server 2012 All Editions
   5. Microsoft Windows Server 2008 R2 SP1 All Editions

G. Virtual Environments: Operation on virtual environments shall be supported. Software security and piracy protection shall be done using a means that allows a virtual environment to be transferred between hardware platforms with restriction. The use of Software Serial Numbers (SSN) and internet based registration is required.

H. System Server: The software program shall consist of multiple servers including, but not limited to, Database and Communications Server, and Client Workstation. The Servers shall be capable of being installed on one or more PCs across a network providing a distribution of system activities and processes.

I. The access control and security management system shall use a non-proprietary open SQL database engine to store and share information. The software program shall be compatible with the following versions of Microsoft SQL Server in either Standard, Enterprise, or Express editions:
   1. SQL Server 2012
   2. SQL Server 2008 R2
   3. SQL Server as supported by the manufacturer
J. Database: The database architecture shall be Microsoft SQL Server 2012 as standard and provide the capability to utilize Microsoft SQL Server 2008 R2 if required.

K. Communication: The system shall have the capability to communicate with the integrated access control and alarm panels via LAN/WAN connections utilizing industry standard TCP/IP communication protocol, EIA-485 Isolated Serial Communications or Dial-Up Modem Interface Connection. The system shall provide encryption of all data transmitted from the communication server. The system controller must have an Ethernet connection onboard and not installed as an ancillary or third-party interface device.

L. System Accounts/Database Partitions: The system software shall allow support for multiple partitions allowing separate access to ALL components of a site. The system shall provide a global partition for use by all partitions. Users, Schedules and Access levels shall be global to allow for easy administration and be able to be assigned to individual System Controller(s). The global users, access levels and schedules shall be capable of being used by multiple controllers and can be assigned to any local access level or schedule.

M. Languages: The system shall support the installation of multiple language versions. The language versions currently available include:

1. English
2. French
3. French (Canadian)
4. Estonian
5. Greek
6. Italian
7. Romanian
8. Polish
9. Russian
10. Spanish

N. The system programming shall be user friendly, and capable of being accomplished by personnel with no prior computer experience. The interface shall utilize drop boxes for all previously entered system-required data.

O. Online Help: The programming shall be MENU driven and include online "Help" or "Tutorial" information, as well as online data entry examples. The Help shall be available by using the F1 key. When using the F1 help access, the help menu shall provide detailed information relative to the operation that the user is performing without the need to key in additional search parameters.

P. Hardware Configuration: After installation, the Owner shall be able to perform hardware configuration changes. These hardware configuration changes shall include, but not be limited to, door open time, door contact force time, door, input and reader names, when and where a cardholder is valid, and the ability to add or modify card databases as desired without the services of the Contractor or manufacturer.

Q. Hardware Enclosure: The system shall be supplied to meet installation within a standard 19" rack mount environment, DIN rail mounting or standard enclosure and PCB style mounting. The use of any one of these shall NOT prevent the other form of enclosure being used within the same system where more suitable or at the request of the owner. The control panel shall be provided with system monitored tamper alarm and an internal panel cover that conceals all the wiring and terminals except for DIN norm LED Status indicators. Hardware shall be compatible across the different form factors.

R. Equipment Repair / Replacement: Equipment repair shall be able to be accomplished on site, by module replacement, utilizing spare components. A minimum of one spare component of each module or remote device shall be provided.
S. Distributed Processing: All control components shall utilize "Distributed-Processing" concepts. The distributed processing shall include the ability to download operating parameters to any system controller, thus allowing the system controller to provide full operating functions independent of the integrated access control system computer.

2.3 OPERATOR SECURITY LEVELS

A. Assigned passwords shall be possible to define the levels of system operation for each individual operator. System operation for individual operators shall include, but not be limited to, restricted time periods for login, available accounts and default language selection at login. Operator actions range from no view or control rights to basic monitoring to full control of the system including programming. Operator access shall be defined by Security Levels and Records Groups assigned to a role.

B. When creating a new role, The SMS shall provide four preset operator levels. Presets shall provide a quick means of providing operator access and cannot be edited. The SMS enables the ability to create additional security levels to customize access to meet your specific requirements.
   1. Administrator: Can perform all actions in all sites without any restrictions
   2. Installer: Can perform actions required to install and configure the system
   3. End User: Can perform reporting and limited system configuration for users
   4. Guard: Monitoring of the system and viewing of events only

C. Operator restrictions shall be able to facilitate:
   1. Multi-tenancy buildings using one or more controllers and a shared server.
   2. Multiple branches that need to securely restrict site access to appropriate branch operators while allowing complete visibility for security personnel.
   3. High-security installations with multiple departments or facilities where restricted operator access is required to prevent the assigning of access levels containing restricted doors or floors to users with insufficient security clearance.
   4. Using Security Levels and Record groups, operators shall be able to restrict access to the following items within the software application.
      a. Users
      b. Access Levels
      c. Door Groups
      d. Floor Groups
      e. Controllers
      f. Doors
      g. Elevator Cars
      h. Elevator Groups
      i. Door Types
      j. Input Types
      k. Areas
      l. Schedules
      m. Menu Groups
      n. Phone Numbers
      o. Reports

D. The software application shall prevent any logged in operator from viewing details on any alarms or events, triggered by a system component that they do not have access to view.
2.4 SYSTEM CAPACITIES

A. The following section specifies the maximum capacities that can be achieved when using the SMS system:
   1. Unlimited Users
   2. Unlimited Access Levels
   3. Unlimited Door Groups
   4. Unlimited Doors
   5. Unlimited Alarm Area Groups
   6. Unlimited Schedules
   7. Unlimited Floor Plans
   8. Unlimited Status Pages

B. Server/Workstation
   1. The system shall require one master control file server and be able to support a minimum of 20 additional concurrent (logged on) control locations, photo identification stations, or workstations, utilizing LAN/WAN network software and hardware.
   2. Workstation licenses are concurrent and determined by the total number of logged in clients.
   3. Workstation software can be deployed on any workstation limited only by the server licensing restrictions.

C. Web Client
   1. The system shall be able to be accessed via the SMS web client. The web client shall use the SMS SOAP Service to access and display the application within a web environment.
   2. As a minimum, operators shall be able to view the following from the web client:
      a. Live and historic events
      b. User records
      c. Reports
      d. Status Pages
      e. Door Groups
      f. Area Groups
      g. Output Groups
      h. Elevator Groups
      i. Floor Groups
      j. Schedules
   3. It shall be possible to run multiple web client instances simultaneously.

D. Installation: The system software shall be capable of being installed on any workstation provided that the licensing requirements are not violated. Only the number of users allowed by the licensing agreement shall be permitted to be logged on at any given time.

E. Hardware Security Device: The system software shall not use any hardware security device (dongle) for the server or workstation components. Security of the software shall be provided by a software serial number used at the time of installation and by the registration of the system server component.

F. System Control: Overall management of the access control and alarm monitoring shall be through software, which provides complete integration of the security and access control components. The system shall not rely on the operation of the server, workstation or other external computer component to make or action decisions on access control.
G. File Server Communication Download: The file server shall be able to operate with or without the communication of hardware and support downloading of changed or modifications only.

H. Backup Modem Connection: The backup modem connection shall operate with the same specifications as that of the direct Ethernet connection however limitations on the speed of transfer may be applicable.

I. Modular Expansion
   1. The system shall offer one Server License package that is expandable in modular increments to total capacity. The software shall support modular licensing for key portions and in minimal and large increments. Additional communication server licenses shall be made available to expand the system capacity as needed. Upgrading a user license or the number of communication servers shall not require any additional software.

   2. The Security Management System Server License shall include:
      a. 50 Doors
      b. Unlimited Sites
      c. Unlimited Controllers
      d. Unlimited Users
      e. 1 Concurrent Client
      f. 1 Cameras
      g. Unlimited VMSs
      h. Calendar Actions
      i. Photo ID
      j. Email on Event
      k. SOAP Web Service
      l. Web Client and 3 Web Operators

J. Firmware Updates: The firmware of all devices shall be updatable. The firmware of the ISC and the expansion modules shall be updatable from the web UI.

K. Software Updates: Regular software updates shall be available from the manufacturer and shall be simple to apply.

2.5 CONTROLLER

A. The system shall be configured with the application software connected via Ethernet to one or more system controllers.

B. The system controller shall be the central processing unit responsible for the control of security, access control and intrusion detection in the system. The system controller shall be designed with industry standard DIN Rail Mounting.

C. The system controller shall be available in three main editions. The controller shall:
   1. IP enabled – IPv4/v6 supported.
   2. Certified for Access Control and Intrusion detection
   4. Maintain Access Control and Intrusion functions in case of loss of communication with the server.

D. Standard SMS Controller: The standard system controller shall include the following:
   1. 10/100 Ethernet interface
   2. Encrypted module network using RS-485 communication
3. Communication with Ethernet modules that are interconnected using a LAN or corporate network
4. In-built offsite communications dialer (ContactID, SIA)
5. 32 Bit advanced RISC processor with 2Gb total memory
6. 8 high security monitored zone inputs
7. 1 high current monitored bell output
8. 2 high current Form C relay outputs
9. 2 reader ports, configurable for either Wiegand or RS-485 reader operation
10. The ability to connect 2 readers using the independent reader inputs or use the 2 reader operation to connect 4 readers providing dual entry and exit door connection

E. Controller Capacities: The controllers shall be able to support the following varying capacities:
1. 200 Keypads
2. 4,000,000 cardholders
3. 248 Input Expanders
4. 64 Reader Expanders
5. 32 Output Expanders
6. 32 Analog Expanders
7. 5288 Inputs
8. 9152 Trouble Inputs
9. 2956 Outputs
10. 128 Doors
11. Unlimited Areas
12. Unlimited Schedules
13. Unlimited Users
14. 128 Floors
15. 8 Elevator Cars
16. 248 Smart Readers
17. 50000 offline events

F. Controller Communication
1. The system shall be built around a central server and one or more controllers. The server shall be responsible for maintaining the system configuration and monitoring, while the control panels shall be responsible for the physical control and operation of the system. While the control panels are designed to run standalone, network connectivity is required between the central server and the control panels to enable configuration and monitoring.

2. Communication between the controller and the server shall be encrypted, ensuring data integrity between the control panel and the server. Encryption shall rely on a shared key that both the control panel and the server know. The message is encrypted using the key, then decrypted by the receiver using the same key. If the control panel and the server have different keys, the message shall not be able to be decrypted. This shall result in the rejection of incoming messages.

3. The system Controllers shall have a high resilient architecture with support for multiple paths, minimum three, to communicate with the Event Server.

4. Communication between controllers shall be facilitated by cross controller operations. Cross controller operations shall enable controllers to operate as one system and share hardware resources. This shall make all physically connected items on a controller accessible and usable by various functions and records within the application software. Cross controller operations shall happen behind the scenes where controller communications shall be automatically established when items belonging to different controllers are assigned to the same record within the application software.
G. Power Modules

1. The system power supply modules shall communicate system voltages, current, status of electronic fused outputs, core temperature and fault conditions back to the Security Management System. The power supply modules shall charge backup batteries and report low battery alarm. Relay outputs only for low battery and fault conditions shall not be acceptable.

2. The power module shall be able to:
   a. Have mains input ideal for reducing complexity in set up and ready deployment of module
   b. Support 2 Form B Relay outputs that can be used as programmable outputs while the module is online, or as additional status outputs for monitoring battery failure/disconnection and AC failure when the module is offline or in standalone mode
   c. Have battery backup connection for continued power delivery in power outage conditions
   d. Use Intelligent charging algorithm that monitors battery and AC supply allowing optimum performance
   e. Relay information about critical system voltages, currents and core temperature to the SMS software
   f. Include High-performance 32-Bit processor
   g. Support Industry standard DIN Rail mounting

H. Reader Expander

1. A two-door reader expander must be available with two reader ports that shall be able to support either RS-485 or Wiegand reader interfaces. The reader expander shall support the configuration of the independent reader ports to control two doors for entry or exit, or the configuration of the independent reader ports to control two doors with entry and exit connection.

2. The reader expander shall be able to:
   a. Monitor the door position
   b. Support the connection of a REX (Request to Exit) or REN (Request to Enter) switch
   c. Control an electronic door lock
   d. Operate in offline mode using All Users and First 35 Users plus 150 Card Cache
   e. 2 reader ports, configurable for either Wiegand or RS-485 reader operation
   f. The ability to connect 2 readers using the independent reader inputs or use the 2-reader operation to connect 4 readers providing dual entry and exit door connection
   g. Support intelligent reader tamper operation

I. Input Expander

1. A hardware module must be available to monitor up to sixteen independent input devices and shall be available in either full or half DIN sizes.

2. The input expander shall be able to:
   a. Have any combination of normally closed or normally open input devices connected
   b. Use analog and digital processing with 5 over sampling
   c. Use 4 state input alarms using resistors to provide short, alarm, closed and tamper conditions
   d. Support 4 Form C relays capable of switching resistive loads up to 7 Amps
   e. Include a high-performance 32-Bit processor

J. Input / Output Expander
1. A hardware module must be available to monitor up to eight independent input devices and four output devices.

2. The input expander shall be able to:
   a. Have any combination of normally closed or normally open input devices connected
   b. Use analog and digital processing with 5 over sampling
   c. Use 4 state input alarms using resistors to provide short, alarm, closed and tamper conditions
   d. Support 4 Form C relays capable of switching resistive loads up to 7 Amps
   e. Include a high performance 32 Bit processor

K. Output Expander
   1. A hardware module must be available to monitor up to eight independent output devices and shall be available in either full or half DIN sizes
   2. The output expander shall be able to:
      a. Monitor 8 Form C relays capable of switching resistive loads up to 7 amps
      b. Indicate the relay state for all relays on board
      c. Include a high Performance 32 Bit processor

L. F/2F Reader Expander
   1. A hardware module shall be available to provide sites using legacy end-of-life Casi-Rusco hardware and those operating F/2F card readers, with a seamless migration path to Security Expert.
   2. The F/2F reader expander shall be able to:
      a. Provide 8 reader ports using the F/2F protocol
      b. Provide the ability to simply unplug the existing Casi-Rusco Secure Perfect/Picture Perfect or GE/Micro5 reader connection and fit to the Security Expert F/2F reader expander
      c. Monitor door position contacts and request to exit devices over standard F/2F protocol

M. LED Indicators: All DIN Rail modules must have front panel LED indicators to display the status of the device for diagnostic purposes.

2.6 CARD READERS, CARDS & KEYPADS

A. The card readers shall read encoded data from cards, tags or remotes and send the data back to the system. The card reader shall give an audible and visual indication of each read. Different audible tones shall be used to distinguish between a successful and denied credential reading.

B. Range of Card Readers
   1. Multi Card Technology: The range of card readers shall be available with either 125kHz proximity or 13.56MHz smart card capability or as a multi technology reader that combines both capabilities in a single unit.
   2. Clone Card Detection: The card readers shall provide built-in clone detection when using Schneider Electric Secured MIFARE. This means that even though it is possible to copy a single MIFARE credential, use of that copied credential shall be detected and prevented when a reader with clone detection is used.
   3. Clone card detection shall operate in the following modes:
      a. Clone Card Read: The Clone Card Reading option shall determine whether a clone card has been detected but will continue normal operation.
b. Clone Card Notify: The Clone Card Notify option shall enable the reader to notify the reader expander if a card presented is a clone card. This option shall require the Clone Card Read option to also be enabled.

c. Clone Card Destroy: The Clone Card Destroy option shall enable the reader to modify a card so that it can no longer be read if it is determined to be a clone card by the reader.

4. Flexible Communication: The Schneider Electric range of card readers shall provide the capability to use an RS-485 reader interface, or a Wiegand interface.

   a. The RS-485 reader interface shall provide fast, flexible, secure communication with the added benefits of being easier and more cost effective to wire and deploy. The RS-485 protocol shall be bidirectional to ensure that the reader is in constant communication with the controller. This shall prevent replaying the data stream to gain access and shall ensure that any interference with the reader cabling will be detected quickly. Using the bidirectional protocol shall also enable the ability to use encryption between the card reader and the controller. When this is paired with an encrypted DESFire card solution, it shall provide a fully encrypted communication path right from the card to the server. The RS-485 reader interface shall allow cable runs of up to 3000ft (900m).

   b. The Wiegand reader interface shall provide compatibility with all standard access control systems. The Wiegand reader interface shall allow cable runs of up to 500ft (150m).

5. Multiplex/Multidrop

   a. The RS-485 reader interface shall support multiple wiring configurations. The RS-485 reader interface shall allow both home run and multidrop wiring configurations, providing the ability to use existing cabling on system upgrades and keep cabling costs to a minimum on new installations.

   b. Both the RS-485 reader interface and the Wiegand reader interface shall allow the ability to connect two readers using the independent reader inputs or use the two reader operation to connect four readers providing dual entry and exit door connection.

6. Situational Awareness: The Smart Readers shall provide visual indication of security posturing of the facility through programmable functions by the SMS system. Smart Readers shall be configurable to display different colors, multiple color sequences across multiple colors from the RGB spectrum based upon automated or manual commands from the SMS or Control Panel(s).

7. IP65 Protection: The Schneider Electric series of card readers shall have the IP65 environmental rating to provide a high degree of protection from the elements. Readers shall be mountable indoors or outdoors.

C. Card Reader Technology: The card reader system shall support multiple card reader technologies including:

1. Proximity
2. Wiegand
3. Biometrics
4. Magnetic stripe
5. Bar Code
6. Keypad
7. Card/keypad (PIN)
8. High-speed long-range Vehicle ID
9. Smart Card (MIFARE or similar open formats)

D. Keypads: The Keypad system shall be compatible with a range of keypads that shall be capable of:

1. Arming and disarming areas
2. Door Control
3. Viewing user areas
4. Monitoring the status of any door, user (anti-passback), inputs, outputs and schedules
5. Supporting Offline functions that allow quick key menu functions to be performed on objects used for automation (lights, HVAC, electric gates and doors)
6. PIN code operation with support for 1 to 8 digit user codes
7. Activating 3 reportable panic events (panic, medical and fire)

E. The keypad system shall be compatible with the following keypad models: The SMS Touch Sense LCD Keypad

2.7 SECURITY MANAGEMENT SYSTEM MOBILE APP

A. The system shall be compatible with the Security Management System Mobile App. The Security Management System Mobile App shall be capable of:
   1. Arming and disarming areas
   2. Door Control
   3. Monitoring the status of inputs and outputs
   4. Displaying live events with the ability to search and filter events
   5. Providing a mobile access credential to unlock doors using NFC / Bluetooth
   6. Viewing the live video feeds of IP cameras that allow direct URL access to either a static JPG image feed or a streaming MJPG video feed
   7. Sending push notifications that provide system and sensor activity

2.8 INTERCOMS [- NOT USED]

A. The intercom range shall offer an open standard, no-proprietary solution that can operate as a standalone point-to-point intercom system or integrate with The SMS for complete capability and efficiency.

B. VoIP compliance shall allow for:
   1. Complex call routing, enabling communication to multiple stations at once
   2. Calls to be routed to alternative stations if they are not answered
   3. Calls to be diverted to different units based on a schedule

C. Within the interface, integration shall allow:
   1. The ability to add intercoms to floors plans for monitoring the status of the intercom and for making and receiving calls
   2. The ability to link intercoms to doors to enable operators to communicate with a visitor before granting access remotely
   3. A variety of listening and viewing options

D. Power over Ethernet (PoE) models shall be able to simplify installation and reduce costs by eliminating the time and overhead associated with AC outlet installations, while providing flexibility of the install location.

2.9 17” ENTRY STATION [- NOT USED]

A. The SMS Entry Station shall be able to operate as a standalone unit, or as part of a complete integrated SMS solution. The entry station shall provide an intuitive interface for visitors to communicate with tenants, building management, a concierge, or even to off-site locations, such as directly linking guests...
with corporate housing owners. VoIP and video capability enables you to view live video from multiple sources and utilize two-way voice communication to SIP compliant phones and intercoms.

B. VoIP compliance shall allow for:
1. Complex call routing, enabling communication to multiple stations at once
2. Calls to be routed to alternative stations if they are not answered
3. Calls to be diverted to different units based on a schedule

C. The entry station shall:
1. Provide user integration with The SMS to enable the management of tenancy directory listings within Security Expert. Directory listings shall automatically synchronize and display on the entry station
2. Allow communication with any Security Expert controller to control any connected physical devices and monitor the status of the entry station. When integrated with Security Expert, certain functions can be programmed that enable a user to use the entry station to unlocks doors, trigger lighting or call an elevator
3. Provide local door control using the onboard open collector output
4. Be configurable via a web interface
5. Provide an optional postal lock for complexes or buildings with mailboxes on the secure side of the installation
6. Provide a live video feed that is viewable from a remote monitoring station, a web browser, a Grandstream IP phone or from within the SMS
7. Be built with a vandal resistant body and stainless steel front plate to protect against malicious damage
8. Accommodate surface, flush and kiosk mounting

2.10 ADDITIONAL SYSTEM HARDWARE

A. Motion Detectors: The system shall support motion detectors to prevent false alarms.

B. Wireless Products: The wireless product range shall include a variety of wireless button remotes and a wireless receiver for simple integration with alarm and access control systems.

C. Enclosures: All module hardware components (controllers and expanders) shall be housed in lockable metal cabinets that are fitted with tamper switches and meet the appropriate environment requirements. The control panel shall be provided with system monitored tamper alarm and an internal panel cover that conceals all the wiring and terminals except for LED status indicators.

D. DIN Rail Enclosures
   1. All DIN Rail enclosures shall have:
   2. A removable door for simple mounting
   3. Space provided above and below the DIN module location for finger trunking
   4. Cable tie points for secure, clean wiring
   5. An internal cover window for protecting the wiring
   6. A variety of sizing options
   7. A range of flexible mounting options

2.11 SYSTEM CAPABILITIES

A. The system shall operate as a true client server application where multiple clients are able to connect to a single serve. All databases shall have the ability to ADD, DELETE, VIEW or EDIT information
The system shall provide storage of all system events and operator transactions in a retrievable form and made available through industry standard ODBC or SQL connection. The usage of proprietary database formats shall not be acceptable.

B. The system shall log all events by time and date (log time) and log all events by time and date of when the event occurred at the hardware (field time). The system shall provide the capability export selected system transactions to the clipboard or disk file by activation of an export button, configuration of an event filter, operation of an external application that generates a file. The System shall provide ability for Owner to make system configuration changes such as, but not limited to door open time, door unlock time, door name, reader names, when and where a cardholder is valid, and the ability to add or modify card databases at any time.

C. Duress feature shall operate when a PIN is used that has been set as a duress user or the user has entered a PIN incremented by one number from their PIN number.

D. Two User Rule: In instances where two valid, non-identical users must be used within a programmable time period to grant access to an area or door, a user shall be able to be configured as either a provider or master dual custody user.

E. The system shall be able to display when a card holder who uses the reader has accessed (opened) the door or if the card was used but the door was not opened.

F. The system shall enable latch mode operation, where the first valid card read unlocks the door and the second causes it to lock the door.

G. The system shall provide hardware system diagnostics that can easily be selected, clearly showing system configuration or commands not accepted by any of the attached hardware components.

H. An indication of the hardware status shall be shown clearly on the status bar of the client application.

I. The system shall provide ability for manual operator control of system outputs. The manual functions shall include the ability to energize, de-energize, energize for time, or energize on pulse the output relay. The pulse time shall be a programmable setting with specific on and off rates of duty cycle.

J. The system shall provide ability for manual operator control of system doors. The manual functions shall include the ability to Lock, Unlock, Disable Exit, Disable Entry and Exit, Unlock Latched.

K. The system shall automatically display stored "video image" of cardholder when a door pop up window is shown with a live view and archived view of the associated camera.

L. The cardholder "video image" pop-up shall be activated based on the door configuration. The size of the pop-ups shall be adjustable by the operator.

M. The system shall provide a means for scheduled automatic backups of any or all database system files. A means to restore these files using standard SQL Server Management Studio or similar shall be provided.

N. The system shall provide the ability to communicate with modems using windows TAPI and have the configuration of modems and their function (Dial-Up, Dial-In, Alarm Only, SMS Output) within the system.

O. Communication from the access control communication server to the remote intelligent control panels shall use TCP/IP communication and shall be part of the control panel. The software and server shall not be restricted in anyway by the number of hardware devices it can communicate with.

P. All commands and updates to the panels shall be verified and shall automatically retry if communications have failed. In the case a panel fails to receive communications an event shall be activated.
Q. All programming of information to the system controllers shall occur automatically with the option to enforce a manual download selectable per controller.

R. Display the online status of the controller and the last download status: Date and time of the last download shall be saved in the controller. The last IP address that the controller communicated to the server on shall be logged in a Last IP Address entry in the controller record.

S. The system shall provide the ability to initiate a page to a paging system based on a received event condition. An event condition shall be defined as any event and MUST not be limited to controller based events.

T. A host grant mode of operation shall exist that requires the host computer to grant accesses to "valid" cards. An alternate host grant mode shall allow the card access information to be downloaded along with unlocking the door for "valid" cards.

U. All database records shall have a history that is displayed when opening the record, the history shall show each change on the record and shall include but not be limited to, the operator name, time of change, type of transaction and what changed in the record with the old and new configuration.

V. All database records shall have a quick shortcut to the events within the system database filtered by the record.

W. Access Control
   1. Dual Authentication: The system shall allow the configuration of a door such that it can only be opened if two valid cardholders present their access badge at the door within a defined time period. This mode shall also allow for supervisory access (e.g.: visitor escort) and an override function based upon cardholder so that cardholders of an authorized level do not require a subsequent cardholder before entry is permitted.
   2. Two Factor Authentication: The system shall allow the configuration of two factor authentication. Two factor authentication shall enable a card holder to use both a physical credential (card, remote or tag) and a PIN code to unlock a door from a card reader. This shall prevent a lost or stolen credentials from being used to gain unauthorized access.
   3. Anti-Passback
      a. The system shall provide support for anti-passback control. Anti-passback control shall ensure that a user that has used their card at a door’s entry reader will not be able to re-enter through the same door until they have exited through a defined exit reader.
      b. The anti-passback control shall also be flexible so that cardholder’s that have violated anti-passback rules or have lost their access card can be forgiven by a system operator.
      c. Anti-passback modes shall include hard (no forgiveness), soft (allows access but generates an alarm event) and timed for all readers on the intelligent controller, on specified reader or card for a definable period of time.
      d. Anti-passback shall have the facility to be reset by a timed schedule.
   4. Offline Operation: The system shall enable reader expanders to operate in offline mode when connection with the controller is lost. Reader expander shall operate in offline mode using All Users or First 35 Users plus 150 Card Cache.
   5. Door Types: The system shall support door types. Door types define how a door will operate. The system shall support the default door and shall also support the created of new, custom door types. This includes the passback mode, the reading mode used to gain access (such as Card, PIN, Card or PIN, Card and PIN, etc.), and if operator verification is required to grant access.
   6. Slave Doors: The system shall support the configuration of slave doors. Slave doors will follow the primary door when it unlocks and locks. This can be used to lock / unlock internal office doors automatically when the main entry door is locked or unlocked.
7. Door Interlocking
   a. The system shall allow the configuration of a set of interlocked doors, such that opening any single door within the defined set prevents any other door from being opened at the same time, even if a valid cardholder attempts to gain entry at that door.
   b. In addition, it shall be possible define a time period once the first door has been closed, before another door in the set can be opened.

8. Door Lockdown: The system shall enable the configuration of door lockdown that can be applied to a single door or an entire site to restrict entry, exit or all access during an emergency situation.

9. Emergency Egress: The system shall enable the configuration of an emergency egress function to unlock a single door, create an egress path, or unlock the entire site to facilitate a smooth emergency evacuation.

10. Extended Access Time: The system shall enable the configuration of an extended access time for particular users to make their way through selected doors.

X. Intrusion Detection

1. Area Counting: The system shall allow the configuration of area counting to track and monitor the number of users within a certain area. This information shall enable the system the automatically arm when the last person leaves the area, or restrict access to the area if the user count has been reached.

2. Child Areas: The system shall allow the configuration of child areas. Child areas shall follow the parent area when it arms and disarms.

3. Configurable Input Types: The system shall enable the configuration of default and custom input types. Input types instruct inputs what to do when they are triggered. Multiple input types shall support a range of detection devices for motion, panic and smoke.

4. Disarm Delay: The system shall support Disarm Delay. Disarm delay can be used to deter armed robberies. Once a user requests an area disarm a delay timer is started.

5. Dual Code Control: The system shall allow the configuration of Dual Code Control. Dual Code Control requires two authorized users to enter PINs to disarm a restricted area.

6. Configurable EOL: The system shall support configurable EOL to save on time when upgrading from an existing system. The system shall enable an operator to easily select the EOL value that the old system use.

7. Automatic Rearm: The system shall allow an area to automatically arm once it has been disarmed for a period of time. This can be used the limit the time a user can remain in an area for.

8. Duress Alarm: The system shall allow a user to arm or disarm an area as normal, but when a dress code is entered, or a duress button is pressed, the system sends a silent alarm to the offsite monitoring station.

9. Stay Arming Mode: The system shall allow the perimeter of the building to be armed while the occupants are free to move around inside the building.

10. Loiter Areas: The system shall allow the configuration of loiter areas. Loiter areas can be used to ensure that users do not remain in a transit area for an extended period of time. Loiter Areas can only be used with Anti-Passback enabled and must use entry and exit readers on all access points.

11. User Areas
   a. The system shall allow individual areas to be assigned to users.
   b. The user area can be used to disarm the selected area automatically on login to a keypad or when access is granted at a door or reader. This feature is ideal for securing many individual offices yet arming all of them when all employees exit and disarming only the person's office that they are allowed to access while other offices remain secure and protected.
Y. Users

1. The following section details the requirements for the operation of the user database and configuration parameters.
   a. Cardholder information shall include unique card number up to 15 digits and optional Personal Identification Number.
   b. Allow multiple cards per cardholder. Minimum shall be 8 card holder records.
   c. Provide an unlimited number of user definable fields that can be set to.
   d. Provide an unlimited number of user definable tabs.
   e. Provide special card options that include, but are not limited to:
      1) Time zone reference, which defines valid time.
      2) Display of a greeting message to a user when logging in to a keypad.
      3) Provide an option to take the user directly to keypad menu options when logging in to a keypad.
      4) An extended activation time on doors for physically impaired users that is programmed per user and per door.
   f. Provides a specified activation date/time and expiration date/time (spanning years)
   g. Provide a card "Trace" function. The Trace function shall allow normal access control but shall provide a tracking event at the system monitor.
   h. Provide ability to store digital image of cardholder and use the digital image to generate identification cards, transaction information and user reports.
   i. Upon editing card information, the updated information shall be sent automatically to the appropriate access control panel with no other user intervention. If the port is dial up, the entry shall be stored locally and shall be updated when connection is re-established.
   j. Card numbers 0 and 65,535 shall not be valid card numbers when assigned to a user as some devices transmit these numbers on an improper read or as part of a high-level card reader process.
   k. Provide a special report option that is directly within the user (tab) that will generate an event report based on all events associated with the user.
   l. Must have a graphical view of the access that a user has to doors and alarm areas displayed as a list of doors with a seven day schedule. A green bar will indicate access at the time it is shown.

2. User Search
   a. The system shall enable operators to generate one off user, door, and access relationship reports.
   b. A User Search generates a 'one-off' temporary report that can be printed but cannot be saved. To create reports that you wish to run again at a later date, use the additional user reports functionality.
      1) All Users
      2) All Users who have Access to the selected Doors
      3) All Users included in the following Access Levels
      4) All Users by Events
      5) All Users by Record Group
      6) Users by Event Type/Doors
      7) Cards about to expire
      8) Lastest Users through Door(s)
      9) All Users NOT in Events
      10) All current visitors
      11) All overdue visitors
12) All visitors by Date

3. User Images
   a. The system shall enable you to capture photos using digital webcams directly from the SMS interface for added efficiency and convenience, or select an existing photo from a local or network folder. Size and crop them to best fit the ID card design.
   b. Photos are displayed in the event window against user events and are also visible when using the SMS Web Client. Use the photo stored against a user to provide validation when a user badges at a door. This enables an operator to perform a live comparison before allowing entry.

4. User Violations
   a. The system shall be able to monitor each card that is presented to each reader connected and will ensure that access is prevented under any of the following circumstances:
      1) The user does not have access to disarm the armed area behind the door
      2) The user is trying to unlock a door or enter an area outside of a defined schedule
      3) The user is trying to unlock a door or enter an area that they do not have permissions for
      4) The user record has expired in the system
      5) Anti-passback rules have been violated
      6) The card has been presented at a reader before the user record’s start date, or after the user record’s end date.
   b. Any user violations shall be reported in the event log.

5. User / Card Inactivity
   a. The system shall enable the configuration of the following automatic actions after a set period of days, hours or minutes has elapsed with no activity:
      1) Disabling a specific user card
      2) Disabling a user record
      3) Deleting a user record

6. User Import: The system shall support the importing of multiple users at one time. As entering data manually can be tedious and data entry is often prone to human error, the system enables you to use the generic CSV file format to import user information. CSV files can be generated from many ERP systems and can even be created from a Microsoft Excel spreadsheet. The columns within the spreadsheet can be mapped to fields within the SMS user tables.

7. Expired Users: It shall be possible to add an expiry date to a user record to prevent certain users from being granted access when they are no longer authorized to. When a user record has expired, it remains in the system.

8. Custom Field Tabs: The system shall provide a function for creating custom user information. This function shall enable the ability to add the following information types to the user menu:
   a. Text
   b. Numerical
   c. Time
   d. Date
   e. Time and Date
   f. Option
   g. Link
   h. Drop Down Box
   i. Image

Z. Groups
1. Door Groups: The following section details the requirements for the operation of the door groups and configuration parameters.
   a. Door group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any door using a drag and drop window to the door group.
   c. Door selection will be filtered by the record group and only show the doors under the record group.
   d. Set a schedule for any programmed door in the door group.
   e. Display the controller name that the door is located on in the door group and in the selection window.
   f. Provide tree structure for records that are grouped using the record group configuration settings.
   g. Usage information must be shown in a tab listing the location of all places that reference the Door Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

2. Area Groups: The following section details the requirements for the operation of the area groups and configuration parameters.
   a. Area group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any area using a drag and drop window to the door group from any controller.
   c. Set a schedule for any programmed area in the door group.
   d. Display the controller that the door is located on in the door group and in the selection window.
   e. Provide tree structure for records that are grouped using the record group configuration settings.
   f. Usage information must be shown in a tab listing the location of all places that reference the Area Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

3. Elevator Groups: The following section details the requirements for the operation of the elevator groups and configuration parameters.
   a. Elevator group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any elevator to the group using a drag and drop window.
   c. Display the controller that the elevator is located on in the elevator group and in the selection window.
   d. Provide tree structure for records that are grouped using the record group configuration settings.
   e. Usage information must be shown in a tab listing the location of all places that reference the Elevator Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

4. Floor Groups: The following section details the requirements for the operation of the floor groups and configuration parameters.
   a. Floor group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any floor to the floor group using a drag and drop window.
c. Display the controller that the floor is located on in the floor group and in the selection window.
d. Provide tree structure for records that are grouped using the record group configuration settings.
e. Usage information must be shown in a tab listing the location of all places that reference the Floor Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

5. Menu Groups: The following section details the requirements for the operation of the elevator groups and configuration parameters.
   a. Menu group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any keypad group using a drag and drop window.
   c. Provide tree structure for records that are grouped using the record group configuration settings.
   d. Usage information must be shown in a tab listing the location of all places that reference the Menu Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

6. Keypad Groups: The following section details the requirements for the operation of the floor groups and configuration parameters.
   a. Keypad group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any keypad to the keypad group using a drag and drop window.
   c. Display the controller that the keypad is located on in the keypad group and in the selection window.
   d. Provide tree structure for records that are grouped using the record group configuration settings.
   e. Usage information must be shown in a tab listing the location of all places that reference the Keypad Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

7. Output Groups: The following section details the requirements for the operation of the floor groups and configuration parameters.
   a. Output group names shall consist of an entry that allows a custom name of up to 250 characters.
   b. Provide the ability to assign any output to the output group using a drag and drop window.
   c. Display the controller that the output is located on in the output group and in the selection window.
   d. Provide tree structure for records that are grouped using the record group configuration settings.
   e. Usage information must be shown in a tab listing the location of all places that reference the Keypad Group. This reference list shall not need to be specifically run or executed and be shown in a grid view when selecting the tab.

8. Record Groups: The following section details the requirements for the operation of the record groups and their configuration parameters.
   a. Record groups must allow the assignment of any name to the record group.
   b. Multi nested record groups will display as branches and sub branches under the parent record group as a tree.
   c. An ICON will show an expandable record group when displayed or a folder.
d. Record groups can be assigned to the following records;
e. Users
f. Access Levels.
g. Door Groups
h. Floor Groups
i. Controllers
j. Doors
k. Elevator Cars
l. Elevator Groups

AA. Access Levels
1. The following section details the requirements for the operation of the access levels and configuration parameters.
   a. Provide the ability to define a specific scheduled operation time for the access level to allow the assigned user access to the programmed resources.
   b. Provide the ability to assign resources to the access level with a drag and drop selection using the following records;
   c. Assign any number of door groups from the configured door groups.
   d. Arming Area Groups that allow the user access to the Alarm Areas to Arm Only.
   e. Disarming Area Groups that allow the user access to the Alarm Areas to Arm and Disarm the Areas.
   f. Assign specific elevator cars.
   g. Assign a floor group that the access level will grant access to.
   h. Provide a template of a defined access level, where changes can be made to the template and saved as a new access level. The number of templates shall not be limited and will be able to be copied from when adding new access levels.
   i. Provide an access control tree structure for records that are grouped using the record group configuration.
   j. Usage information must be shown in a tab listing the location of all places that reference the Access Level. This reference list shall not need to be specifically run or executed and be shown in a grid like view.

BB. Photo ID and Image Verification
1. The system shall provide Photo ID capabilities that enable an operator to design, produce and encode professional looking cards. The interface shall provide the operator with full control over the information that is included and the card design can be customized to accommodate corporate branding. Image verification of user is carried out by comparing the person photograph stored in Security database and live video feed from camera system integrated the security management system. Photo ID must be provided as standard feature of the Security management system. It must not be separately licensed option.
2. Card Template Editor
   a. The card template editor shall provide an extensive range of formatting options for designing and creating templates. The card template editor shall enable operators to define the layout and information used when producing cards:
      1) Add and format text
      2) Include images such as company logos or backgrounds
      3) Add placeholders for user details such as photo, name, card number and barcode
b. There shall be no limit to how many card templates can be created

3. User Photos
   a. The system shall enable operators to capture photos using digital webcams directly from the user interface or select an existing photo from a local or network folder.
   b. User photos shall be displayed in the event window against user events and shall also be visible when using the SMS web client.
   c. The ability to add user photos shall also enable operators to validate a user’s access when they badge at a door. This allows operators to perform live comparisons before granting entry.

4. Card Encoding: If using a supported printer, operators shall be able to encode cards, or print and encode cards in the same operation from within the user interface.

CC. Record History
   1. The system shall allow operators to view the changes made to individual records. The record history shall display:
      a. When the record was initially created
      b. Which operator created the record
      c. When and if the record has been changed
      d. Which operators have changed the record
      e. What about the record has been changed

DD. Record Usage: The system shall allow operators to view where records are being used within the interface.

EE. Building Automation: The system shall be capable of facilitating building automation integration through the use of a Smart Connector IP level integration and also support communication protocols such as BACnet and MODBUS. The integration shall allow operator interaction form the building automation system the ability to make intelligent decisions based and allow for remote control of doors and security system points/objects. Security Management System controller must support Modbus and BACnet industry standard protocols for integration with other compatible building technology systems.
   a. Interact with, control doors/portals for open, close, lock down and monitor.
   b. Interact with security points for activate, deactivate and monitor.
   c. Visually display system device statuses from within the Building Automation system.
   d. Provide point level visibility to allow the interaction with lighting management systems to come on progressively as staff arrive and turn off as they leave
   e. Provide point level visibility to allow the control of HVAC system devices to enable/disable when rooms/areas are occupied/unoccupied to support the significant reduction in energy use and greater cost savings
   f. Activate lighting in low occupancy areas (such as restrooms and storage areas) only when sensors detect motion
   g. Control lighting based on areas that employees onsite are allowed to access
   h. Set lighting to adjust to full power when cleaners arrive in the evening to ensure good visibility
   i. Turn off non-essential items automatically when the alarm is set at the end of the day, and on again when the alarm is deactivated
   j. Configure HVAC systems to maintain a lower temperature when a building is unoccupied and increase to a comfortable temperature as people arrive for the day
   k. Turn off air conditioning when a window is opened, then back on when the window is closed
2. The Security Management System shall be able to control these functions directly via output modules or through integrations with third party systems using the C-Bus, Modbus, BacNetIP protocols and the Schneider Electric Smart Connector protocol.

FF. Proximity Solutions: The system shall provide support for various proximity solutions using 13.56MHz smart cards. 13.56MHz smart cards offer a high level of security and greater functionality:

1. Multiple Vendor Credentials: The 13.56MHz range of proximity cards and tags shall support multiple vendor credentials. The Schneider Electric secure credential shall be loaded into one sector of the card, leaving the remaining sectors open to be encoded with any credentials from other vendors. This ability shall allow the use of one card seamlessly access areas on site that may be controlled by more than one system.

2. Dual Format Cards: Incorporating low frequency (125kHz) and high frequency (13.56MHz), dual format cards shall allow the same card to be used to access both low and high security doors. Dual format cards shall also provide a smooth migration path for organizations that wish to transition to smart technology.

3. Data on Card: The data-on-card functionality offered through 13.56MHz technology shall enable offline locking systems to read, receive and write information via smart cards. Data shall be captured from cards at online hot spots located at strategic points around the building and the hot spot uploads and downloads user related information to the access control system. Changes are written to the card and quickly spread through the system as the card is presented at each offline lock.

4. Follow Me Printing: The functionality of 13.57MHz smart cards shall enable the secure printing of documents. Follow Me Printing holds a user’s print job on a server until the user authenticates the job at a printing user their card or tag. This shall enable the setup of printing jobs in advance, and enable the ability to save money, reduce wastage of uncollected paper and prevent potentially sensitive information from falling into the wrong hands.

5. Cashless Vending: 13.56MHz cards shall be capable of being programmed with a monetary value for use with a cashless vending system, making them ideal for businesses where an unattended payment system is required such as:
   a. Academic campuses
   b. Laundromats
   c. Libraries
   d. Apartment buildings
   e. Carparks
   f. Sports facilities
   g. Cafeterias

GG. Schedules and Holidays: The following section details the requirements for the operation of the schedules and scheduling process

1. Schedule definitions shall include Starting time, Ending time, Days of the week, and Holiday override.

2. The maximum number of periods defined within a schedule shall not be less than 8 and allow for at least 8 holidays per period.

3. Time shall be definable in 24-hour (military) time.

4. The minimum number of schedules that can be assigned to a panel shall be 1024.

5. A schedule must have the ability to assign a name that is at least 256 characters in length.

HH. Calendar Actions: The system shall provide the ability to create Door and Output Calendar Actions that override previously programmed Schedules for a specified duration. Calendar Actions shall be able to be configured as one-offs or set them to recur every day, week, month or year. Calendar Actions must
be provided as standard feature of the Security management system. It must not be separately licensed option.

II. Function Codes: The system shall provide the ability to specify a single key-press Function Code (0-9) plus credential sequence at a specific reader to allow a user to perform a specific function, e.g. to arm an Area or latch unlock a Door. Any manual commands possible in the software shall be possible with a Function Code.

JJ. Credential Types: The system shall be able support credentials such as license plates and bar codes. The third-party device or software used to collect the credential data shall be configured as a smart reader with the data being sent through to the controller via the onboard RS-485 reader ports or via Ethernet. This feature shall support Unicode, UTF8, ASCII, Numeric, Hexadecimal, Wiegand and TLV data formats.

KK. Graphical Floor Plans: The software program must use Graphical Display Icons (GDI) for representing hardware devices, system controllers and remote modules in the system. The icons shall be used in floor plan pages and plan views to provide the user interface to control and monitor the system. The devices when placed on a plan must be capable of being viewed as an ordered list in a separate window or column on the same page or by selection of a display list or option. Selecting a display list shall not change the floor plan display. The GDI's must have a minimum of 30 default icons representing various objects and devices. The GDI's must support an unlimited number of custom end user GDI's. A GDI must be created using standard XAML or similar OBJ type file. The following section details the requirements for the operation of the floor plan and graphic display.

1. Provide the ability to import floor plan graphics stored in a JPG or BMP format.
2. Provide the ability to link background images to a local or network folder.
3. Provide the ability to associate all GDI's to floor plan graphics allowing the user to control and monitor the system.
4. Provide the ability to link floor plan graphics together in a hierarchy fashion or by the use of buttons on individual floor plans.
5. All of the floor plans are to be viewed as a list showing all GDI's as a list in hierarchical order.
6. Associate graphical icons with devices to control and monitor the system
7. Display the real time status of devices and objects on your system
8. Using event filters and alarms, you can jump to a floor plan based on an alarm condition or trigger

LL. Status Lists: The following section details the requirements for the operation of the status list that can be applied to any pane of a status window and allow an operator control.

1. Provide the ability for dynamic updates of the status in real time on the system computer client display.
2. Provide color and status text details specific to a status device.
3. The control tree shall be created by the user and allow for manual control of all system devices. By right clicking on a device in the tree the operator be able to initiate the appropriate action from a pick list.
4. The control tree in a status list shall allow the addition of any combination of types and not be limited to a specific type. The mixing of doors, outputs, inputs, and areas shall be possible within a status list.
5. The status list shall add an optional filter that can be assigned to ONLY show the status of a specific device. It shall be possible to display only doors that are forced open as an example hiding other door status from the list.

MM. Status Pages
1. The system shall allow the creation and customization of status pages to provide an intuitive graphical interface. The flexible design shall enable operators to include the content relevant to a particular site to display a sitewide overview.

2. The Status Page Editor shall enable an operator to include any combination of:
   a. Status lists that dynamically update to display the real time status of attached devices
   b. Floor plans that display a visual representation of the site and the real time status of devices
   c. Live video feeds from an integrated VMS/NVR camera
   d. Event reports filtered to include only the events you wish to view
   e. Variables that return information on changeable data such as room temperature or humidity levels
   f. Web pages displaying the contents of a defined website or locally stored HTML page
   g. Muster reports that displays a list of all users within a specified area

NN. Events

1. All events shall be logged by time and date that the event occurred in the software application and when the time and date that the event occurred at the hardware.

2. The ability to create customizable event filters shall enable operators to sort and filter what and how event information is displayed to improve efficiency and ensure an accurate response to incidents.

3. The system shall allow:
   a. The creation of event filters that match a particular record or event type
   b. The ability to filter status lists by status, such as open doors or areas that are armed
   c. The ability to color code Event types to make particular types of events stand out to an operator
   d. The ability to display User images inside live event and alarm windows
   e. The ability to configure emails to be sent when a certain event occurs.

2.12 ALARMS

A. The system shall support manual responses to alarms entering the system. Each alarm shall be capable of initiating a number of different actions, such as activation of remote devices, door control and activation of WAV files.

B. All events within the system MUST be configurable as an alarm and MUST have individual messages with each event.

C. The following section details the requirements for the operation of the alarm monitoring and alarm view window operation:

1. Report alarm point activity.
2. Provide a color for an alarm that has been triggered, configurable from the alarm window.
3. Provide the ability to access the default floor plan graphic for any active alarm point by right clicking the alarm.
4. Provide ability to bypass inputs in the system to prevent an alarm.
5. Execute alarm notification in all modes of operation.
6. Provide ability to acknowledge any alarm, card, or reader activity based on priority.
7. Provide display of system activity with the higher priorities displayed at the top of the list with an unlimited number of priority options.
8. Provide ability for the operator to acknowledge and clear alarms from display. Prior to acknowledgments, the user shall be allowed to enter a response per alarm. The system shall offer a means to require acknowledgment of an alarm before it can be cleared.

9. Provide a display of the most current transactions in real time.

10. Provide the ability for dynamic alarm monitoring of alarm points in real time on the system computer's video display terminal.

11. Provide an alarm view filter that is structured as a list allowing the operator to select individual devices or groups of devices to be viewed and assigned to any configurable alarm or event window.

12. Provide a trouble condition and associated event warning the operator that the communications within the system has been disrupted and provide a means to display this to an operator.

13. Provide a "Panel Communication Fault" alarm if communication to a panel is lost.

14. Provide real time printing of alarms using a right click selection for creating an immediate real time report.

15. All events within the system MUST be configurable as an alarm and MUST have individual messages with each event.

16. Provide mode of system operation that requires the operator to enter a response to an event when acknowledging it from the alarm view window.

17. Provide mode of system operation that allows acknowledged alarms to be automatically cleared.

18. Provide mode of system operation where unacknowledged events will cause the computer to continuously play an audio file and display an alarm notice until all unacknowledged alarms are acknowledged. A momentary silence feature shall allow the audible tone to cease for up to 60 seconds on the selection of the alarm window. The status bar will show the total number of alarms in the system and a shortcut button that will take the operator to the alarm list window.

19. When an acknowledged, but not cleared event is in the alarm log it will be reissued automatically requiring acknowledgment when the event changes to an alarm or trouble condition.

20. Provide mode of system operation that does not allow the operator to clear an alarm prior to it being restored to normal.

D. Alarm Events: Alarm events with defined priorities shall be able to pop-up automatically in an Alarm event window for operator attention. The pop-up shall display the name of the event (reader, alarm point, cardholder or system alarm), time, date, site, account, the card number (if a card event), type of event and cardholder name. An event counter shall also display the number of times the event was reported to the Alarm event monitor prior to Acknowledgment or Clearing the event. Event instructions shall be made available by double clicking on the event.

E. Custom Alarm Event Window: The Alarm event window shall allow the operator to initiate a physical response to the event as well as a written response. Responses shall include but not be limited to: acknowledge, clear, open a pre-programmed floor plan, energize, de-energize, pulse, time pulse, add comment, retrieve event video, shunt/bypass or un-shunt/remove bypass.

F. Alarm Priority: An Alarm priority is not limited and shall be a numerical list configurable by the end user. An alarm priority can be assigned to any alarm and determines the order by which an alarm is displayed.

G. Alarm / Zone Input Display: The system shall provide both supervised and non-supervised alarm / zone monitoring. Upon recognition of an alarm, the system shall be capable of switching a floor plan. The system shall be capable of arming or disarming an area containing alarm / zone inputs both manually and automatically, by time of day, and by day of week.

H. Alarm Routing: Alarm Routing enables you to define which workstation groups alarms are sent to and the sequence in which they are routed. This allows you to route an alarm to specific workstations rather
than all workstations at once, and to transfer an alarm to another workstation if it is not acknowledged within a defined timeframe.

2.13 ACTIONS

A. The system shall enable the creation of actions to trigger a process that runs automatically when specific events occur. For example, sending a command to a VMS to increase the frames recorded per second when the system detects that a door is forced open.

B. Actions shall have the following functions:
   1. Save to Database to save a record of the event
   2. Send PTZ Command to send a PTZ command to a VMS
   3. Popup Camera Window to display a live camera feed for the event in a popup window
   4. Run Script reserved for future use to run a custom script
   5. Send Email to send an email to a specified email address
   6. Send Event to create an xml version of the event that is then sent to a third party system
   7. Custom VMS Action to send a custom command string to certain VMS systems that the VMS will then react to
   8. Delete Visitor Card reserved for future use to allow automatic signout and cancelation of visitor cards at specified readers
   9. Send Event to MSMQ to transmit the event to a queue using Microsoft Message Queuing (MSMQ) which can then be read by third party systems

2.14 REPORTING

A. The following section details the requirements for the operation of the reporting utility and filter operation:
   1. Direct transaction reports shall be provided in a tab and shall be available on but not limited to Users, Doors, Inputs, Outputs and Areas and when selected will give the operator the ability to generate the latest 500 transactions filtered by the selected record. Transactions will be displayed as an ordered list in a grid view or as a formatted view that allows as you type filtering on any text or transaction information.
   2. Direct transactions will support the selection of a print preview that will show the filtered result of the records. All print previews shall allow printing to an installed printer. Export to the following file formats (PDF, Excel, TIF, JPG, PNG, HTML, RTF, XML and CSV) must be supported.
   3. Provide reporting capability for printing of selected system transactions from the database for any range from time and date to time and date.
   4. Provide feature to generate a transaction report for an alarm point(s) state. An alarm point state shall be defined as Open, Closed, Tamper and Short.
   5. Provide feature to generate a history report of system alarms. A system alarm state shall be defined by panel connected and include any transaction event from the panel.
   6. Provide feature to generate a history report for a user either directly from the main transaction tab or from the event view option in the user menu.
   7. Provide feature to generate a transaction report for system operator(s) activities. The report shall include time, date, operator name the device associated with the action and the type of action performed by the operator. Activities shall include but not be limited to:
      a. Acknowledged and cleared alarms, door control, record editing or adding, input bypass, module and network updates, any and all manual commands on a device.
   8. Provide complete database reporting of all data programmed into the system data files that allows the direct export of the data from the record using the Clipboard or a specific CSV generated file.
   9. The system shall provide the tools necessary for the operator to create custom reports.
10. The system shall provide the ability to export reports to a local or network file location periodically or based on a set time / day.

B. The following report types shall be available:

1. Event Reports: The Event Report feature shall provide the ability to view a group of events that can be customized and filtered to show only relevant events. Events in Event Reports shall be loaded continuously as the report is being executed and while the report is filtered or reordered.

2. User Reports
   a. The User Report feature shall provide the ability to view detailed information on the users / cardholders within the SMS. Reports can be filtered to display the following:
      1) All Users
      2) All Users who have Access to the selected Doors
      3) All Users included in the following Access Levels
      4) All Users by Events
      5) All Users by Record Group
      6) Users by Event Type/Doors
      7) Cards about to expire
      8) Lastest Users through Door(s)
      9) All Users NOT in Events
     10) All current visitors
     11) All overdue visitors
     12) All visitors by Date
     13) All modifications made to user records
   b. Additional sorting filters shall also be available for each report type.

3. Muster Reports: The Muster Report feature shall provide the ability to generate a report that will list all users present within a specified area. Muster reporting feature shall be integral part of the Security Management system base software and must not be separately installable application.

4. Time and Attendance Reports
   a. The Time and Attendance Report feature shall provide the ability to record the entry and exit of users at designated card readers or groups of card readers.
   b. Time and Attendance shall be integral part of the base software and shall not be a separately installable application.
   c. The Time and Attendance Report feature shall support the configuration of custom reports. Custom reports will enable an operator to specify shift rotations, overnight shifts, break times and applicable public holidays.
   d. The Time and Attendance Report feature will support the following report types:
      1) Daily First In Last Out
      2) Shift First In Last Out
      3) Daily First and Last User Event
      4) Shift First and Last User Event
      5) First Scan In
      6) Last Scan Out
      7) First Scan In and Last Scan Out
      8) Late In
      9) Top 10 Late In
     10) Late Out
     11) Early In
     12) Early Out
     13) Absent
     14) Top 10 Absent
5. Central Station Reports: Central Station Reports shall provide a report map for the Contact ID and Report IP services that can be supplied to a monitoring station. Reports shall be generated for individual controllers.

2.15 ELEVATORS

A. Low Level Elevator Integration: The system shall allow low level integration with elevator systems to provide floor access control. The system shall be able to:
   1. Provide the ability to apply schedule to floors for scheduled unlocking/locking
   2. Provide the ability to automatically lockdown the floors and elevators in an emergency lockdown situation
   3. Provide the ability to automatically unlock the floor and elevators in an emergency egress situation
   4. Provide the ability to configure either fail-safe or fail-secure operation following power loss or a system restart.
   5. Provide the ability to unlock the floors a user has access to once the user has entered the elevator car and presented their credential at a card reader
   6. Provide the restriction of only enabling one floor to be selected when a user presents their credential at a card reader. This shall prevent unauthorized users accessing floors that they have not been assigned permissions for.
   7. Provide the ability to configure Destination Reporting in cases where an audit trail of users and the floors they have accessed are required

B. High Level Integration: The system shall provide support for industry leading 3rd Party elevator destination dispatch systems through IP level integration. Integration shall only be performed from the IP level controller and not be required to leverage server side functions.

2.16 DIRECT CAMERAS

A. The application software shall support the monitoring of IP cameras that allow direct URL access to either a static JPG image feed or a streaming MJPG video feed.

2.17 MONITORING

A. The system shall support traditional analog monitoring (Contact ID and SIA) and IP monitoring (Report IP).

2.18 PANEL

A. The following section details the requirements for the hardware integrated control panel unit connecting to the communication server.
   1. Provide ability to program all functions of the system locally using a LCD keypad module attached to the system.
   2. Provide ability to program descriptions, shunt times, and momentary shunt times for all system alarm points.
   3. Provide ability to program descriptions, pulse times, and energize times for all system output relays used for door control and other auxiliary functions.
   4. Provide ability to program descriptions for all system card readers.
   5. Monitor both supervised and non-supervised alarm points with the ability to select by point which point shall be supervised and define if the point is a normally closed or normally open point contact.
   6. Provide ability to interlock any alarm point condition to an output relay.
7. Provide ability to interlock any alarm point condition to another alarm point.
8. Provide ability to interlock any alarm point to switch a camera to a system monitor.
9. Provide ability to program alarms and associate incoming alarms with related outputs.
10. Provide a programmable "delay" setting up to 255 seconds for all system alarm points.
11. The system shall not report the alarm condition until the delay setting has expired.
12. Under no circumstances shall a site code limitation exist for any card reading device or reader expansion module. Multiple format card reading must be supported across all panels and devices.
13. Support up to 128 readers per Intelligent Control Module.

2.19 VISITOR MANAGEMENT [~ NOT USED]

A. The following section details the Visitor Management features that shall be integral part of the Security Management system base software and not a separately installable application:
1. Enable users to register and track your visitors directly from the interface,
2. Streamline Sign In & Checkout process
3. Customize the user experience
4. Allow Real Time Monitoring and Reporting

2.20 NETWORKING

A. The following section details the requirements for the operating of the TCP/IP Network and communication server.
1. Provide networking capabilities (LAN or WAN) as a standard feature, as defined by licensing, not as an installed software upgrade or physical hardware add on component.
2. Provide 1 Server and licensing for up to 1 user workstation configurations. Licensing may be purchased at a later date for the required number but must not be limited to any value below 1.
3. Provide the ability for a network system to support concurrent users up to the maximum limit. Example, one workstation adding cards and making user changes, another workstation monitoring alarms, yet another running database reports, another controlling door openings and alarm functions, and so on.
4. The workstation shall have the same GUI (graphical user interface) functionality as the workstation that operates on the server machine.

2.21 WEB CLIENT

A. The system shall be able to be accessed via the SMS web client. The web client shall use the SMS SOAP Service to access and display the application within a web environment. The SOAP Service shall be installed on the same machine as the SMS server, or on a separate physical server.

B. As a minimum, operators shall be able to view the following from the web client:
1. Live and historic events
2. User records
3. Reports
4. Status Pages
5. Door Groups
6. Area Groups
7. Output Groups
8. Elevator Groups
9. Floor Groups
10. Schedules

2.22 THIRD PARTY INTEGRATION

A. VMS/NVR Systems: Digital Video Recorder (VMS) or Network Video Recorder (NVR) models must be directly integrated and displayed within the front end interface.

1. Support shall be provided for the following makes and models as a minimum:
   a. Pelco
   b. Exacq Vision
   c. Panasonic
   d. Axxon
   e. Arkiv
   f. HikVision
   g. Mirasys
   h. Avigilon
   i. Onvision
   j. Milestone
   k. DVTel Latitude
   l. Geutebruck GCore
   m. Geutebruck Geviscope

2. Support must be provided for the following:
   a. Live Video display must be shown as a pane or window in a status page with the ability to show 16 different images from any combination of VMS or Camera.
   b. Archived view will be accessed directly from the workstation user interface and provide the same functionality as the client view of the VMS manufacturer.
   c. Linking of ANY event to an archived video stream will be achieved using the assignment of the camera to an event or the assignment of the camera to an event filter.
   d. PTZ commands shall be supported that can be activated on an alarm automatically switching a PTZ controlled camera to a specific pre-set associated with the alarm condition.

B. Locking Solutions

1. The system must provide the ability to integrate with various online and offline locking solutions.

2. Salto SHIP
   a. The system shall provide high level integration with Salto SHIP and shall enable the seamless combination of online and offline doors.
   b. Salto SHIP integration shall provide the ability to:
      1) Control online and offline locks within SMS software
      2) View accurate and searchable audit trails of online and offline events
      3) View archived footage from all related cameras
      4) Monitor wireless doors in real time
      5) Encode cards in a single operation from within the SMS interface

3. Salto SALLIS
   a. The system shall provide integration with Salto SALLIS.
   b. Salto SALLIS integration shall provide the ability to:
1) View real time access control and event monitoring
2) View an online audit trail and battery status
3) Reduce installation costs
4) Communicate with the system using Ethernet or RS-485
5) Support Escutcheon and Cylinder lock types

4. Aperio
   a. The system shall provide integration with Aperio wireless locks.
   b. Aperio integration shall provide the ability to:
      1) Support Escutcheon and Cylinder lock types
      2) View an online audit trail and battery status
      3) Reduce installation costs
      4) Communicate with the system using Ethernet or RS-485
      5) View real time access control and event monitoring

5. Cencon
   a. The system shall provide integration with Cencon ATM and Vault locks
   b. Cencon integration shall provide the ability to:
      1) Provide centralized user management of ATM/Safe locking devices
      2) Combine access control, intrusion detection, and ATM security
      3) View accurate audit trails and transaction logs
      4) Manage Cencon smart keys from a SMS workstation
      5) Create Cencon users and Cencon lock groups

6. Allegion
   a. The system shall provide integration with the Allegion AD Series of wireless locks.
   b. Allegion integration shall provide the ability to:
      1) View a live audit trail and battery status
      2) View real time access control and event monitoring
      3) Communicate with the system using RS-485
      4) Extend the reach of access control to areas where running wires is not suitable
      5) Simplify installations by combining the electrified lock, status monitors and reader into one device.

7. VingCard
   a. The system shall provide integration with the VingCard VisiOnline system.
   b. Vingcard integration shall provide the ability to:
      1) Manage back of house staff access to electronic hotel locks directly from the SMS interface
      2) Provide a wireless locking solution that controls electronic hotel locks
      3) Use the users and access levels in SMS to verify credentials in the VingCard VisiOnline system.

C. Motion Detection
   1. The system must support integration with various third-party motion detection systems.
   2. Redwall
      a. The system shall be able to integrate with Optex Redwall laser scanners.
      b. Integration with Optex Redwall laser scans shall provide to ability to:
1) Detect the size, speed and distance of moving objects
2) Extend the reach of intrusion to areas where running wires is not suitable
3) Monitor the state of the detectors within the SMS
4) Reduce false alarms and guards call outs

3. **Inovonics**
   a. The system shall be able to integrate with the range of Inovonics wireless detections units and mobile duress devices using the Inovonics Wireless Receiver Module in conjunction with the Inovonics EN4200 Echostream repeater.
   
   b. Integration with Inovonics devices shall provide the ability to:
      1) Simplify installation by utilizing wireless technology
      2) Extend the reach of intrusion to areas where running wires is not suitable
      3) Monitor the state of Inovonics devices using trouble inputs

### 2.23 BUILDING MANAGEMENT SYSTEMS

A. The system must support the integration with Building Management Systems to control HVAC, lighting, energy, fire and elevator solutions. Integration shall be supported by the C-Bus lighting, Modbus TCP, BacNet/IP protocols and the Schneider Electric Smart Connector.

B. The two systems shall support hardware connectivity so that the BMS server is notified when a user locks or unlocks a door, an area is armed or disarmed, a schedule goes valid or invalid, or when motion is detected. The information passed to the BMS server shall be used to make intelligent decisions about what to change and when to change it. The integration shall also enable the BMS to communicate the status of the building to allow SMS to control access.

### 2.24 INTERCOM SYSTEMS [- NOT USED]

A. The system shall allow integration with SIP compliant intercom systems to provide a full featured communication solution. Workstations can be configured to register as a SIP client which shall allow direct communication with IP based intercoms. SIP compliance shall allow for:
   1. Complex call routing, enabling communication to multiple stations at once
   2. Calls to be routed to alternative stations if they are not answered
   3. Calls to be diverted to different units based on a schedule

B. Within the interface, integration shall allow:
   1. The ability to add intercoms to floors plans for monitoring the status of the intercom and for making and receiving calls
   2. The ability to link intercoms to doors to enable operators to communicate with a visitor before granting access remotely
   3. A variety of listening and viewing options

C. The SMS shall also be able to integrate with serial intercoms using the Intercom service. This shall provide a direct link to Siedle, Sentex Infinity Multi Point, Sentex Infinity Single, Enterphone, SES and MESH intercom solutions. The Intercom service shall allow automatic token generation for elevators, doors and other control functions.

### 2.25 ELEVATOR SYSTEMS [- NOT USED]

A. The system shall be able to integrate with destination based elevator management systems using a high level interface to provide a complete multi-floor access control solution.

1. Support must be provided for the elevator management systems:
   a. **KONE**
b. OTIS  
c. Schindler PORT  
d. ThyssenKrupp  
e. MCE  

2. The system shall have control of the access permissions assigned to users and the schedules that the elevators run to.  
3. The system shall be used to verify a user’s request to access a floor (through access levels, schedules or area status) and grants or denies the request. When a user’s request is verified, the elevator system shall direct them to the elevator that will provide them with the shortest travel time to the floor.  
4. The system shall communicate with the elevator management systems via Ethernet.  
5. The integration shall not require the need the wire relays or inputs between the two systems.  
6. The system shall only require a small amount of programming in order to interface with an elevator management system.  
7. The integration shall provide synchronization between the two databases to reduce data entry and administration time.  
8. User access events shall be logged to provide an accurate audit trail.  
9. The integration shall provide the ability to control floor access from the Security Expert interface.  

2.26 BIOMETRICS [- NOT USED]  
A. The system must be able to be integrated with Suprema Biometric Readers.  
1. Biometric readers shall be connected using a standard open Wiegand interface.  
2. The system shall be used to authenticate access using the data from the biometric reader.  
3. Readers shall support life detection to prevent unauthorized access.  
4. For greater security, a biometric reader can be combined with an access control reader to require dual authentication.  

2.27 ELECTRONIC KEY CABINETS [- NOT USED]  
A. The system must be able to be integrated with KeyWatcher Touch keyboxes.  
1. KeyWatcher Touch system operation shall be synchronized with new and existing users, access levels and schedules within Security Expert.  
2. Integration between the systems shall allow the reporting functionality available within the SMS to be used with the events and alarms available with KeyWatcher Touch.  
3. Available keys shall be linked to a SmartKey containing an identification chip that shall enable a user to access the KeyWatcher Touch cabinet and have Smart Keys released or returned.  

2.28 DATA SYNC SERVICE  
A. The system must be able to use the Data Sync Service to pull and transfer to and from third party data sources.  
1. This shall provide the ability to synchronize data between the systems to reduce management time and administration while providing a single point of data entry. This integration shall be ideally suited for:  
   a. 24-hour gym and fitness centers  
   b. Sports clubs  
   c. University student databases
d. Human resource systems
e. Visitor management systems
f. Freight and delivery services

2. Data shall be extracted from the third-party system and saved to a shared network folder. The Data Sync Service is configured to monitor this folder and automatically import the relevant data into the SMS, creating records (including users, access levels, areas, doors, schedules, and so on) for each matched entity. If information in the import file changes, the service shall update the record in SMS.

3. Using the Data Sync Service shall allow the keeping of accurate records, calculation of access counts, calculation of usage, and the generation of reports.

2.29 SOAP INTERFACE

A. The system must be able to utilize the SOAP Service to provide a wide range of integration possibilities. The SOAP Service shall expose the full functionality of the SMS.

B. The SOAP Service shall provide the ability to:
   1. Build custom interfaces to integrate multiple systems into one solution
   2. Integrate the functionality of SMS into a physical device with buttons to unlock doors and disarm areas.
   3. Send events to accounting systems to manage payments.
   4. Extract enrollment data from student management systems to control student access based on the course they are enrolled in and their current schedule.
   5. Extract data from HR or compliance management systems to add to SMS user records.
   6. Extract time and attendance data from SMS and use it to track staff hours for payroll, student attendance to ensure minimum course requirements are met, or to monitor which users are onsite and where they are for compliance purposes.
   7. Adjust schedules in SMS in accordance to manufacturing schedules in an MRP system to ensure that access is maintained based on rostered production hours.
   8. Use information provided from booking systems to control meeting rooms and shared facilities.
   9. Assign temporary access to delivery drivers by automatically creating a user record with the job number as the PIN and an expiry date that matches the expected duration on site.

2.30 AUTOMATION AND CONTROL PROTOCOL

A. The system must be able to use the Automation and Control Protocol to allow third party automation products such as those provided by Control 4, Crestron, AMX, C-Bus, Savant, OpenRemote and Command Fusion, to communicate directly with SMS controllers. The protocol shall enable an operator to control doors, areas, outputs, inputs and variables anywhere in the system, and to monitor the status of these items then report back if the status of the item changes.
   1. Log in using your usual PIN and access level
   2. Unlock doors and control any output
   3. Arm/Disarm an area in regular, stay, force, or instant modes, and bypass inputs
   4. Automatic notifications when a specified door, area, output, input, or variable changes state
   5. Request the state of doors, areas, outputs, inputs and variables
   6. Automatic notifications of system events (all events or just reportable events)
   7. Logout automatically or after a defined period of inactivity (up to 100 minutes)
   8. One minute lock out after three incorrect login attempts, with every incorrect login attempt recorded by the system
   9. Adjust values of variables in the system
10. Configurable encryption: None, 128, 192, or 256 bit AES
11. Support for TCP/IP connections
12. Control the level of lighting and the temperature of a building a smart phone
13. Acknowledgment packets sent by default (can be disabled if interfacing equipment does not support them)
14. Configurable checksum type: None, 8 bit sum, 16 bit CRC
15. Ability to communicate with third party systems for alarm monitoring

2.31 MSMQ

A. The system must be able to integrate with MSMQ. Integration with MSMQ provides the ability to transmit specific events to a queue using Microsoft Message Queuing. This allows third party applications, services, and processes, to take advantage of real time event connectivity with the SMS Server. The implementation of the MSMQ technology provides a very flexible approach to integration and multiple message queues can be used. The MSMQ actions post the event in an XML format.

2.32 LDAP [- NOT USED]

A. Activate Directory or LDAP (Lightweight Directory Access Protocol) shall be provided as a standard licensed option and achieve the following integration.
   1. A link allowing the review of all AD / LDAP added users.
   2. Automatic import without operator intervention.

2.33 LICENSING STRUCTURE

A. The system shall be structured by an enterprise licensing model that shall allow for simple expansion without runaway license costs. The licensing structure shall ensure that the features expected to be in the system are present such as reports, status pages, floor plans and unlimited users, events, schedules and areas.
   1. The system shall be purchased using either a base license.
   2. Flexible license packs shall be available for doors, cameras, IP connected locking solutions and other integration packages.
   3. The licensing structure shall implement a license cap to prevent high license costs. Total number of licensed doors shall be capped at 1000 and the total number of licensed cameras capped at 500.
   4. The licensing structure shall not include any annual software maintenance fees.

PART 3 - EXECUTION

3.1 GENERAL

A. Examine equipment exterior and interior prior to installation. Report any damage and do not install any equipment that is structurally, moisture, or mildew damaged.

B. Verification of Conditions: Examine areas and conditions under which the work is to be installed, and notify the Contractor in writing, with a copy to the Owner and the Engineer, of any conditions detrimental to the proper and timely completion of the work. Do not proceed with the work until unsatisfactory conditions have been corrected.

C. Pre-Installation Conference: Prior to commencing the installation, an onsite pre-installation conference shall review the material selections, installation procedures, and coordination with other trades. Attendees shall include, but shall not be limited to, the Contractor, the Installer, manufacturer’s
representatives, and any trade that requires coordination with the work. Date and time of the pre-installation conference shall be acceptable to the Owner and the Engineer

D. Beginning of the work shall indicate acceptance of the areas and conditions as satisfactory by the Installer.

E. Install equipment in accordance with reviewed product data, final shop drawings, manufacturer’s written instructions and recommendations, and as indicated on the Drawings.

F. Provide final protection and maintain conditions in a manner acceptable to the manufacturer that shall help ensure that the equipment is without damage at time of Substantial Completion.

3.2 FACTORY ACCEPTANCE TESTING [- NOT USED]

3.3 FIELD QUALITY CONTROL [- NOT USED]

A. Functional testing, commissioning, and first parameter adjusting shall be carried out by a factory-trained manufacturer’s field service representative. This manufacturer’s field service technician shall provide all material, equipment, labor and technical supervision to perform inspection, testing and adjustments to ensure equipment is installed, adjusted, and tested in accordance with the manufacturer’s recommendations and is ready for operation. The manufacturer’s field service technician shall replace damaged or malfunctioning equipment and report to the Engineer any discrepancies or issues with the installation.

B. The manufacturer’s representative shall, upon satisfactory completion of inspection and testing, attach a label to all serviced devices indicating the date serviced and testing company responsible.

C. Quality control services include inspections and tests and related actions including reports, performed by independent government agencies, governing authorities, and the Contractor. They do not include contract enforcement activities performed by the Engineer. Inspection and testing services are required to verify compliance with the requirements specified or indicated. These services do not relieve the Contractor of responsibility for compliance with contract document requirements.

3.4 INSTALLATION REQUIREMENTS

A. Cable Installation
   1. Cable installation, identification and termination shall be performed in accordance with the manufacturer’s technical installation guidance, in addition to the applicable codes above. In the absence of the manufacturer’s recommendations on conductor application, the Contractor shall ensure that the cable selected meets all technical requirements of the equipment to be installed.

   2. Cable size must meet the minimum codes of practice for commercial security or low voltage installation and the larger cable specified shall apply. All data or instrumentation cable must be run in the maximum gauge possible and be an overall shielded type.

   3. All cables shall be run as a single cable run and terminated at either end to the control and remote equipment. Where a join cannot be avoided, a junction box must be used and clearly shown on the AS BUILT drawings.

B. Equipment Termination
   1. Termination of all cables to manufacturer's equipment that requires a screw clamp, rising clamp or push to clip connection shall use a termination lug. The termination lug must comply with the manufacturer's technical installation guidelines and be of suitable gauge and size.

   2. It is recommended that a BOOT LACE, FERRAL or PIN CLIP device is used which requires manual crimping. It is preferred that all installations and termination be made with a LeGRAND type termination tool.

C. Labelling
1. All cables shall be labelled with the appropriate cable identification number as specified in the tender documents. Cable labels shall use a NON-removable label that is covered with a protective clear heat shrink.

2. All terminations to control devices shall have an individual label detailing the termination identifier. All termination identifiers will be recorded and provided on AS-INSTALLED documentation and diagrams.

D. Installation of the SMS shall include the appropriate equipment and shall be performed by a factory-trained Contractor installer. The installation shall be completed to these specifications and project plans as required by the Owner or Contractor. A comprehensive Owner site-planning guide for the SMS shall be provided. Adherence to the specific requirements of this document will assist in ensuring a successful System installation. The installation shall include the following:
   1. Site planning and system configuration of field hardware and SMS.
   2. Complete hardware setup of all system Workstations and peripherals.
   3. Complete configuration of all system Workstations, peripherals and installation of field hardware.
   4. Setup of specific network software configuration requirements.
   5. Badge Design and Screen Format installation and verification.
   6. Complete system diagnostics verification.
   7. Complete system operation verification.
   8. Problem reporting and tracking.
  10. Completion of specific Owner acceptance test plans.
  11. Formal turnover of the specific project installation documentation to Maintenance Service Organization.
  12. Regulated power shall be provided by [Contractor][Owner] with dedicated circuits for the installed System. All circuit breakers shall be properly identified and equipped with a “lock” to prevent inadvertent actuation of the breaker.

E. Implementation: Required planning and coordination of numerous elements and deliverables during the installation and commissioning phases shall be handled professionally and within a specified schedule. This SMS project schedule shall follow a PMP outline and agreed to by the client. Milestone/Task durations are dependent upon contractual and system configuration/functionality requirements and assume all critical path tasks, as required by this schedule, are completed as scheduled by all parties involved.

3.5 FIELD TESTING AND COMMISSIONING [- NOT USED]

A. Operational Readiness Testing
   1. The Contractor shall inspect and test furnished equipment and associated systems for conformance to the contract documents, including equipment manufacturer’s recommendations, and readiness for operation. The test shall include the following as a minimum:
      a. Visually inspect for physical damage and proper installation
      b. Perform tests in accordance with manufacturer's instructions
      c. Perform tests to ensure compliance with Contract Documents
      d. Perform tests that equipment is ready for operation
      e. Touch-up paint all chips and scratches with manufacturer-supplied paint and transfer remaining paint to Owner
   2. Contractor shall submit an operational readiness test report documenting all test results, including all assumptions, conditions, allowances and corrections made during the test. The report shall provide a listing of all modifications and adjustments made onsite to include any settings /
parameters not identified as factory defaults within the equipment’s O&M documentation. The test report shall include a signed statement from the Contractor, installer(s) and the factory-trained manufacturer’s representative(s) certifying that the furnished equipment and associated system have been installed, configured, and tested in accordance with the manufacturer’s recommendations, completely conforms to the requirements of the Contract Documents and is ready for operation.

B. Functional Demonstration Testing

1. Prior to scheduling functional demonstration testing the Contractor shall submit a signed statement from the Contractor, installer(s) and the factory-trained manufacturer’s representative(s) certifying that the furnished equipment and associated system have been installed, configured, and tested in accordance with the manufacturer's recommendations, completely conforms to the requirements of the Contract Documents and is ready for operation.

2. The Contractor shall completely demonstrate the functionality and performance of the equipment and associated systems in the presence of Owner and Engineer, observing and documenting complete compliance with the Contract Documents.

3. A phased test and performance demonstration plan shall be developed and documented by the Contractor under the direction of the SMS Systems Supplier. These requirements shall apply to all system components and software, including, but not limited to all system computers, field controllers, card reader devices, PIN pads, photo imaging system peripherals, CCTV cameras and equipment, and interface capability. The Contractor shall perform the tests and document the results under the supervision and witnessing of the SMS System Supplier. Operational scenarios shall be developed and used by the Contractor to simulate the actual use of the system in the normal environment of the OWNER facility. The SMS System Supplier reserves the right to modify the Contractor’s plan or develop new operational test and evaluation procedures to effectively document system operations.

4. The Contractor shall submit a written report documenting successful completion of functional demonstrating testing including all assumptions, conditions, allowances and corrections made during the test.

3.6 TRAINING [· NOT USED]

A. O&M Training: Onsite training specific to the equipment furnished shall be provided to the Owner’s staff by a factory trained manufacturer’s representative. Training duration shall be sufficiently adequate to cover the operation and maintenance of the equipment and shall consist of not less than [1][2 repeated] session(s) with [12] hours of onsite classroom and hands-on instruction for a minimum of [4] attendees per session.

1. The instructor shall provide sufficient time and detail in each session to cover the following as a minimum:
   a. Theory of operation
   b. Major components of equipment
   c. Operation of equipment
   d. Configurations of equipment
   e. Maintenance, troubleshooting and repair
   f. Replacement of component level parts

2. [The submitted O&M manuals shall be used for training.][Manuals and documentation shall be provided to each participant for training.]

END OF SECTION [28 10 11][13700]

©2019 Schneider Electric. Authorization is hereby provided to specifier or design professionals, other than competitors of Schneider Electric, to copy all or part of this document to prepare a specification or bid for a construction project subject to the Disclaimer Statement provided herein. Schneider Electric, Square D, Modbus, Security Expert and EcoStruxure are
DISCLAIMER STATEMENT

This guide specification has been written and is intended to be used by a professionally qualified specifier and/or design professional. The use of this guide specification requires the professional judgment and expertise of the qualified specifier and/or design professional to adapt or revise the information to the specific needs for the Project and is not intended to be used verbatim as a project specification section without appropriate modifications for the specific use intended. The guide specification must be used and coordinated in accordance with the procedures of each design firm, and the requirements of the specific project. This guide specification is subject to change without written notice by the manufacturer and the manufacturer expressly disclaims any warranty, expressed or implied.