University of Utah Software House C•CURE 9000 Specifications and Minimum Requirements

CCURE 9000 Security and Event Management System
Engineering Specification

Software House makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Software House reserves the right to revise this publication from time to time in the content hereof without the obligation to notify any person of any such revision or changes.

Call Software House at 1-(800) 507-6268 for information and assistance.

TABLE OF CONTENTS

University of Utah C•CURE 9000 A&E SPECIFICATIONS

PART 1 GENERAL

1.1 GENERAL DESCRIPTION

The Security Management System (SMS) shall be an extension of the existing University of Utah Campus Wide CCURE-9000 Access Control System as manufactured by Software House, No Exceptions.

CCURE 9000 is a powerful, flexible, multi-function and object-oriented security and event management system that features a variety of customizable interfaces for maintaining the system and for monitoring the desired secure sites. The SMS shall provide an option to display these management and monitoring interfaces in the native languages of the people using the system. The security and event management system shall be flexible in order to meet specific requirements and quickly respond to evolving security challenges. The SMS shall be a scalable platform, simple and economical enough to support a single site, yet upgradeable enough to manage a multi-site network. The SMS shall use an open, distributed architecture, where database servers could reside in geographically separate locations.

The SMS shall provide extensive information management capability using Microsoft .NET Framework V4.61. It shall operate in a Client / Server configuration on personal computers with a Windows-based platform. Its distributed client-server architecture shall be capable of supporting up to 256 simultaneous clients, multiple types of controllers, and over 20,000 input devices, including cameras and multiple types of card readers. The SMS shall be constructed to be database independent and shall support at a minimum Microsoft SQL Server 2012R2 (Express, Standard, or Enterprise), for data protection, redundancy and manageability.

The SMS shall have true multi-tasking, multiprocessor and remote client support; allowing independent activities and monitoring to occur simultaneously at different locations. The operator workstation (Client) shall be user friendly, employing icon-based menus and providing a mouse-driven interface for system operation and the creation of color graphic maps. The user interface shall be customizable, capable of delivering a unique look and feel without a unique version release. It shall be an intuitive user interface that is similar to Microsoft's Outlook and Explorer with its easy navigation and tree structures. A practical application layout editor shall let users drag and drop any application onto one screen and create a customized hub for all activities via a single "command and control" center.

Field devices such as card readers, alarm inputs, control points, etc. shall be connected to fully distributed intelligent field controllers or directly through a Software Development Kit or Web Services, and be capable of operating without host computer intervention. All objects within the SMS, i.e. doors, readers, time intervals, etc. shall be addressed by a unique name as opposed to point numbering or mnemonics. The SMS shall have badge generation tools to create and manage badges using a graphical interface and convenient query features to manage large numbers of badges.

1.2 SUBMITTALS

1.2.A Shop Drawings

Prior to assembling or installing the SMS, the Contractor shall provide complete shop drawings which include the following:

1. Architectural floor plans indicating all system device locations.
2. Full schematic wiring information for all devices. Wiring information shall include cable type, cable length, conductor routings, quantities, and point-to-point termination schedules.
3. Complete access control system one-line block diagram.
4. Statement of the system sequence of operation.
5. Riser diagrams showing interconnections.
6. Detail drawings showing installation and mounting.
7. Fabrication drawings for console arrangements and equipment layout.

All drawings shall be fully dimensioned and prepared in DWG format using any CAD-based software capable of exporting the format (such as AutoCAD).

1.2.B Product Data

Prior to assembling or installing the SMS, the Contractor shall provide the following:

1. Complete product data and technical specification data sheets that include manufacturer's data for all material and equipment, including terminal devices, local processors, computer equipment, access cards, and any other equipment provided as part of the SMS.

2. A system description, including analysis and calculations used in sizing equipment required by the SMS. The description shall show how the equipment shall operate as a system to meet the performance requirements of the SMS. The following information shall be supplied as a minimum:

    a. Central processor configuration and memory size.
    b. Description of site equipment and its configuration.
    c. Protocol description.
    d. Rigid disk system size and configuration.
    e. Backup/archive system size and configuration.
    f. Start-up operations.
    g. System expansion capability and method of implementation.
    h. System power requirements and UPS sizing.
    i. A description of the operating system and application software.

1.2.C As-Built Drawings

At the conclusion of the project, the Contractor shall provide "as built" drawings. The "as built" drawings shall be a continuation of the Contractor's shop drawings as modified, augmented, and reviewed during the installation, check out and acceptance phases of the project. All drawings

shall be fully dimensioned and prepared in DWG format using any CAD-based software capable of exporting the format (such as AutoCAD).

1.2.D **Manuals**

At the conclusion of the project, the Contractor shall provide copies of the manuals as described herein. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each security system integrator installing equipment and systems and the nearest service representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The manuals shall include all modifications made during installation, checkout, and acceptance. The manuals shall contain the following:

1. Hardware Manuals

   The hardware manuals shall describe all equipment furnished including:
   a. General description and specifications.
   b. Installation and check out procedures.
   c. System layout drawings and schematics.
   d. Manufacturers' repair parts list indicating sources of supply.

2. Software Manuals

   The software manuals shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

   a. Definition of terms and functions.
   b. Use of system and applications software.
   c. Initialization, start-up, and shut down.
   d. Alarm reports.
   e. Reports generation.
   f. Database format and data entry requirements.

3. Operator Manual

   The operator manual shall fully explain all procedures and instructions for the operation of the system including:

   a. Computers and peripherals.
   b. System start-up and shut down procedures.
   c. Use of system, command, and applications software.
   d. Recovery and restart procedures.
   e. Graphic alarm presentation.
   f. Use of report generator and generation of reports.
   g. Data entry.
   h. Operator commands.

i. Alarm messages and reprinting formats.
j. System access requirements.

4. Maintenance Manual

   The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

1.2.E System Commissioning

The University of Utah requires a complete system commissioning and point-to-point checkout process before a project is considered complete. Every single point on the system will need to be tested for both software and system-level verification before the warranty can begin. One of the Contractors primary responsibilities is to make sure every single door, sensor and device is set up, calibrated, and operating properly. If any given device has a problem, it could cause the piece of equipment its associated with not to work properly. During construction, contractor is advised to record system progress and the results of your testing and verification process. Before project closeout, there is a contractual requirement which requires you to turn in reports covering every single device and detailing the checkout process and status. All costs for point to point check out and commissioning must be included in contract price. No additional allowance will be granted to complete this process.

1.3 QUALITY ASSURANCE

1.3.A Manufacturer Qualifications

The manufacturers of all hardware and software components employed in the SMS shall be established vendors to the access control/security monitoring industry for no less than five (5) years and shall have successfully implemented at least 5 systems of similar size and complexity.

1.3.B Contractor / Integrator Qualifications

1. University of Utah Pre-Approved Integrators – Utah Yamas Controls, StruxureWorks, Convergent, Global Security.

2. The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems and have a proven track record with similar systems of the same size, scope, and complexity.

3. The security system integrator shall supply information attesting to the fact that their firm is an authorized product integrator certified with the SMS. A minimum of one technician shall be a Certified SMS installer.

4. The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained and certified personnel capable of maintaining the system and providing reasonable service time.

5. The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.

6. There shall be a local representative and factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for these systems.

1.3.C **Testing Agencies**

1. The SMS shall be tested and listed by Underwriters Laboratories (UL) for UL/cUL 294 for Access Control System Units.

2. The SMS shall be tested and listed by Underwriters Laboratories (UL) for UL/cUL 1076 for Proprietary Burglar Alarm Units.

3. The SMS shall employ a FIPS 197-listed AES 256-bit encryption between the SMS Servers, Clients, and iSTAR Ultra/eX/Edge Controllers.

4. The SMS shall include full support for FIPS 201 initiative:

    a. Ability to customize a system-wide Card Holder Unique IDentification number (CHUID).
    b. Ability to configure custom, extended card formats, including GSA 75-bit Wiegand standard, and to download them to the card access panels.
    c. Ability to use Hashed Message Authentication Codes (HMAC) for medium assurance profile.
    d. Enhanced data fields per the FIPS 201 standard, including Agency Code, System Code, Credential Series and Credential Issue Code.

5. The SMS hardware shall comply with the following regulatory requirements:
    a. FCC Class A.
    b. FCC Class B.
    c. CE.
    d. Canadian Radio Emissions requirements.
    e. Restriction of Hazardous Substances Directive (RoHS) 2002/95/EC.
    f. FIPS 140-2 encryption (certified for the iSTAR Ultra/Edge/eX controllers).

6. The SMS shall support Americans with Disabilities Act (ADA) compliance in door and access operation.

1.3.D **Licensing**

Licensing shall be required for the SMS software. The licensing shall include:

1. Series (Model).
2. Number of online readers.
3. Number of online inputs.
4. Number of online outputs.

5. Number of card holders.
6. Number of simultaneous clients.
7. Number of simultaneous badging stations.
8. Optional Features.

1.4 WARRANTY

The SMS shall be provided with a 14-month product warranty from date of shipment or 1 year from date of registration, whichever is shorter. The SMS Hardware shall be provided with a 5 year product warranty from date of manufacture. Software version upgrades shall be available for no charge during this warranty. The software media warranty shall be 90 days per the C•CURE software licensing agreement.

PART 2 PRODUCTS

2.1 MANUFACTURERS

The SMS shall be the Software House C•CURE 9000 system. The Badging Solution shall be Software House C•CURE ID. The SMS field controllers shall be the Software House iSTAR family of controllers. The hardware manufacturer shall be an ISO 9001:2000 registered company.

2.2 DESCRIPTION

The SMS shall be an integrated system that utilizes a single, industry-standard relational database management system for the storage and manipulation of related data. The SMS shall include a server with operating system and applications software, operator and administrator terminals with appropriate software, hard copy printers and fixed magnetic storage media. The security devices shall communicate with the field panels via a dedicated cable network. The field panels shall communicate to the server via a Fast Ethernet 10/100 or 1 GB, TCP/IP network.

The SMS shall allow for growth and scalability from a low-end or entry level system to a high end or enterprise system by increasing CPU power, memory and database. The SMS shall be modular in nature, allowing system capacities to be easily expanded without requiring major changes to system operation. All defined system data as well as historical information shall be maintained. Customizable user interfaces shall allow management of system information and activity for administrators and operators. The SMS shall include an intuitive .NET based badging solution with a WYSIWYG badge layout editor and GUI for badge design.

2.3 SMS Functionality

2.3.A Partitioning

The SMS shall allow system administrators to separate the creation and viewing of objects into partitions. SMS operators shall be associated with partitions and this shall determine which objects operators have the ability to create and or view. The SMS shall support an unlimited number of partitions.

1. The SMS partitions shall include but not be limited to the following objects:

    a. Personnel
    b. Clearances
    c. Doors
    d. Controllers with all associated hardware (readers, inputs, outputs, etc.)
    e. Video servers with all associated objects (cameras, tours, views, etc.)
    f. Application layouts
    g. Events
    h. Dynamic views
    i. Maps
    j. Reports, forms, results
    k. Holidays
    l. Badge layouts
    m. Queries
    n. Images

2. Through the use of privileges, the SMS System Administrator shall be able to determine which objects are associated with a particular partition. These objects shall then be assigned to System Operators with the appropriate privilege.
3. The SMS shall support a super-user assigned the 'System All' privilege who shall have full access to all objects in all partitions.
4. Any operator shall have the ability to be assigned access rights to any partition. Individual Access rights shall be created and have the ability to be assigned to any users of the SMS.
5. The SMS shall allow objects to be created in any partition. The SMS shall have the ability to grant or remove permission from any object in any partition.
6. The SMS shall provide the ability to move objects from one partition to another partition without the requirement of deleting and recreating.
7. The SMS shall provide the ability to import/export any configured object.
8. The SMS shall support the display of all associated objects contained within a partition.

2.3.B **Enterprise Architecture**

1. The SMS shall provide an Enterprise Architecture, licensable option that allows you to configure multiple Satellite Application Servers (SAS) to communicate with a Master Application Server (MAS). The Master Application Server shall provide a platform for global management of the personnel, video, and access control security objects on two or more Satellite Application Servers (SAS) in an enterprise.

2. The Enterprise Architecture shall work by synchronizing each SAS system's database with the MAS database. The MAS shall contain the global data that is used across every server, such as global personnel records, global clearances, and global schedules. The global data shall be synchronized to each SAS to provide enterprise-wide security. The MAS shall be used to remotely monitor and manage controllers and video servers attached to SAS's in the enterprise, however it shall not support any directly connected controllers or video servers.

3. The MAS shall provide the capability for Central Monitoring of the entire enterprise, using the Monitoring Station application. From a Central Monitoring Station connected to the MAS, the system shall be capable of viewing events, activities, and status of every SAS in the enterprise. Alternatively, you can connect to an individual SAS to monitor that system and its connected hardware. In addition, the MAS shall provide the ability to integrate with external sources via LDAP, XML, CSV or ODBC imports both manually or automatically through scheduled processes.

4. Each SAS shall contain database records for all connected video and access control devices, as well as local personnel, clearances, privileges, and other related data. Each SAS shall synchronize with the MAS so that SAS local data is replicated to the MAS for central management and monitoring. In addition, the MAS shall provide central reporting capability for replicated SAS objects including journal and audit transactional data. [Note, for Connected Program integrations, SAS local data is not replicated to the MAS and central reporting is limited.]

5. All local data shall be synchronized immediately to the MAS or queued if a server is offline. All queued data shall be replicated automatically upon restoral of communication. Global data that is created or changed at the SAS/MAS shall be replicated to all locations. Journal and Audit data shall be synchronized either manually or on a configurable schedule, providing the ability to manage bandwidth usage and load balancing.

6. Operators in the enterprise architecture shall be configured as local or global. Global operators shall be subject to the user privileges as defined on each SAS.

7. The Enterprise Architecture shall support a Standalone to SAS Migration Utility that shall be used to merge a standalone SMS server into an existing SMS Enterprise site.

8. The Enterprise Architecture option shall include:

    a. Global Administration of Personnel and Clearances, Images, Card formats, CHUID Formats, Holidays, Personnel groups, and Operators and Privileges
    b. Centralized Reporting
    c. Central Monitoring of Events and Activities across the Enterprise
    d. Central Management of Access Card Enrollment
    e. Central Badging and Image processing
    f. Global Management of Badge Layouts
    g. Single Card Access across the Entire Enterprise
    h. Increased Scalability of Security Hardware and Video
    i. End-to-End Encryption
    j. Automated Synchronization of Enterprise Security Databases
    k. Central Management of Video and Hardware Resources
    l. Remote Editing of Global and Local Data

9. The SMS Enterprise model shall not restrict the addition and/or configuration of over 40 regional application servers configured to a master application server. Testing and qualification has been completed for up to 40 regional servers. However, the SMS shall have no technical restrictions to regional server capacity limits other than system performance.

10. The SMS shall support the configuration of multiple Global partitions in addition to the default Global partition providing the SMS more organization options for objects within the Enterprise system.

11. The Enterprise Architecture option shall provide Multi-Version support. Multi-Version support shall allow SASs running a prior version of the SMS software to continue to synchronize with the MAS allowing for a phased deployment during an Enterprise-wide upgrade. Client connectivity between MAS and Multi-version SASs for monitoring and administration is supported

2.3.C **Graphical User Interface (GUI)**

1. The SMS shall employ a standard Windows graphical user interface (GUI). A mouse and keyboard shall be the primary operator interface with the system. Operator screens shall utilize all standard Windows-style functions such as drop-down menus, context menus, radio buttons, and lists, as appropriate. The interface shall utilize a 'tree structure' similar to Windows Explorer.

2.3.D **Administration Operator Interface**

1. The SMS shall employ an Administration Operator Interface to control the following:

    a. Hardware (readers, inputs, outputs, video systems, door controls, CCTV, and other systems).
    b. Configuration of personnel records, operators and operator privileges.
    c. Graphical Maps.
    d. Application Layouts.
    e. Dynamic Views.
    f. Queries.
    g. Import/Export of objects, including images.
    h. System Variables.
    i. Reports (either periodic or one-time).
    j. System functions (event command and control, actions, schedules).
    k. Display of a list of objects in a grid that can have their values modified and respond to real-time status changes.
    l. Scheduling of backups.
    m. Monitoring of system settings and performance.
    n. Designing of and printing of badges.

2. The GUI shall be configurable by the system administrator to control the views and access of each Monitoring Station operator.

2.3.E **Monitoring Operator Interface / Activity Monitoring**

1. The SMS shall contain a monitoring component that is capable of, among other things, displaying the current state of any object in the system. Additionally the monitoring station shall be capable of displaying a log of all activity that occurs in the system, from object state

changes, to access control information. All text for events (alarms) in the system shall be configurable to be displayed in color based on the user-specified priority of the event.

2. The Monitoring Station shall be capable of showing all changes occurring to an object without requiring the associated activity messages for that object to be routed to that monitoring station. The SMS shall require the operator to have appropriate permissions to view and/or control any object.

3. The monitoring station interface shall be user-customizable. The SMS shall support the ability of the end user to create a customized application layout for the monitoring station. The monitoring station shall support multiple application layouts that can be assigned to the operators. Each application layout can have multiple panes in the same window. The panes can have multiple tabs so that different objects such as cameras and tours can be displayed in the same pane. The panes shall have the ability to include: General activity; Event (Alarm) activity; Dynamic card swipe information; Video cameras and tours; Maps; Dynamic Views; Reports; and links to external applications. Each pane shall have the ability to be moved to a specific screen.

4. The SMS monitoring station shall support a Swipe and Show Viewer. The Swipe and Show Viewer shall monitor a configurable list of Doors, and shall display a portrait or multiple portraits of personnel who present an access credential at a Reader on an included Door or Elevator. The SMS shall allow multiple Swipe and Show Viewers to be added to an Application Layout. The Swipe and Show Viewer shall provide configurable image border colors that shall correspond to access transaction states (Admit, Reject etc.,). The Swipe and Show Viewer shall display the date and time of the transaction, the location, area, Cardholders name and the status of the transaction. The Swipe and Show Viewer shall allow an Operator with the appropriate Privileges to perform the following functions from the Viewer:

    a. View/Edit the Cardholder record
    b. Perform a momentary unlock of the associated door
    c. Grace the Cardholder (allow the cardholder into an APB area)
    d. Perform an Area Lockout Grace of the cardholder
    e. Perform an APB reset on the cardholder

5. The SMS shall support the ability to configure an Operator's Application Layouts to open in separate instances of the Monitoring Station to enhance the performance of multiple displays. Each Application Layout shall support the assignment of a monitor number. The Operator opening the Monitoring Application shall automatically open a separate instance of the Monitoring Application on each assigned Monitor. The SMS shall support up to Ten (10) assigned monitors for Application Layouts.

6. The SMS shall provide the Monitoring Operator with following functional capabilities:

    a. Shall provide a scrolling list of lines or tiles showing current activity on the system.
    b. Shall display activity in real-time as data is being transmitted by field hardware.
    c. Shall include icons that indicate the type of activity and textual description of the activity.

d. The color of the frames of the tiles, icons, and/or text shall indicate the type or importance of the information contained therein.
e. A series of menus, driven by drop-down or trees, shall allow the Monitoring Station operator to perform manual actions, such as “momentary door unlock” for a given door.
f. As part of the manual action capability, the system shall provide screens or boxes that query the operator on specifics, such as start and end time, and offer guidance on performing the manual actions.
g. Ability to view a sortable list of active alarms or events and recently active alarms or activity.
h. Ability to view video from DVMS systems within the same GUI. The video screen GUI shall be able to display multiple panes of live or recorded video and have on-screen camera controls for each live window, providing PTZ control of individual cameras.
i. A GUI that minimizes the number of operator mouse clicks or keyboard strokes.
j. Mouse controls include “right-click” pop-ups and highlighted default selections.
k. Objects shall be displayed to the operator based on his/her assigned operator privilege. The operator shall only be able to monitor/command those objects for which he or she has been assigned privilege.
l. When an operator logs out of a workstation and a new operator logs on, the objects displayed on the workstation screen shall by dynamically updated to display only those objects for which the new operator has privilege.
m. Allow the customization of columns as defined by the operator privilege, including:
    i. Adjusting width (on the fly or pre-programmed).
    ii. Not displaying Columns (on the fly or pre-programmed).
    iii. Sorting on selected columns (to follow standard Windows conventions).
n. Allow for a “freeze” function. This includes a configurable “freeze time-out” that permits an activity to be selected and temporarily prevents the display of subsequent activities which push the selected activity off the screen. A break-through event disables the freeze function. The freeze function shall provide a graphic bar where the remaining time available in the freeze timeout shall be displayed. Selecting the freeze timeout icon before the time elapses shall extend the freeze timeout to the maximum.
o. Provide Acknowledge All, Acknowledge and Clear All and Silence All buttons for events.
p. Support multiple panes for the display of events, activities, video, personnel images, and maps.
q. Display the number of active causes of an event.
r. Support the ability to attach a log message to an event, even after the event has been acknowledged.
s. Provide the ability to attach Predefined Log Messages to an event upon acknowledgement.
t. Shall allow a Monitoring Operator to select on-screen transactions (both events and system activity) and Email the transactions with a single mouse click.

7. Pre-defined Alarm Acknowledgement Messages

The SMS shall provide the ability to create Predefined Log Messages. Each log message shall have a Name, Description, Label and Message Text. These messages shall be assigned to any event providing the ability to select the appropriate response that resolved the event. The SMS shall provide the ability to group multiple log messages and then assign the group to an event. Each group shall contain up to one hundred messages and each event shall support

up to one hundred messages. The SMS shall allow only users with specified operator privileges to add, modify, or delete messages or message groups. Predefined messages shall be editable by an operator with the proper privilege and may be appended as required by the operator.

Messages shall have the following characteristics:

a. Message Name shall be configured with up to 500 characters
b. Message Description shall configured with up to 500 characters
c. Message Label shall be configured with up to 100 characters
d. Message Text shall be configured with up to 3000 characters

8. The SMS shall support audible alarm annunciation at operator workstations (operator configurable audio [WAV] files associated with alarms).

9. The activity monitoring screen shall be capable of displaying the following features:

a. System clock.
b. Date/time when the activity actually occurred and the date/time when the activity was received by the server shall be displayed (when they are different).
c. Real time event counters.
d. Count of the active events.
e. Count of the events requiring operator acknowledgment.
f. Name of operator logged on at the workstation.
g. Real-time display of the current activity on the system in chronological order.
h. Acknowledge All and Silence All buttons for events.
i. Manual Action command buttons.
j. Pre-defined and configurable acknowledgement messages.
k. Log message.
l. Clear event.
m. Clear group of events.
n. Event action message (automatically display selected message for event).
o. Dynamic views.

2.3.F **Web Client**

1. The SMS shall support a Thin Client to provide remote access to the SMS Server via a web browser. The Thin Client shall support Microsoft® Internet Explorer, Safari, Mozilla Firefox® and Google Chrome. The Thin Client shall support 128-bit AES encryption to the SMS Server.

2. The Thin Client shall support Windows Authentication. The privileges of the SMS operator shall be propagated to the Thin Client User allowing only access to Security Objects for which the SMS Operator is authorized. The Thin Client shall provide support for Partitioning of the system and utilize the Partitions assigned to the Operator.

3. All changes made to the SMS database via the Thin Client shall be recorded in the Audit Trail Database.

4. The Thin Client shall provide Personnel Management including:

a. Shall allow the operator to create and modify personnel data (includes adding/removing clearances, schedules, and expiration dates).
b. Operator shall have the ability to enable and disable cards.
c. Operator shall have the ability to search for, edit, add, and delete Personnel records from the SMS database.
d. Search function shall allow wildcards and shall include First name, Last name, card number, and user defined text.
e. Shall support the Auto-increment Card Number feature for Credentials created using the Web Client.
f. Shall support a *Change CHUID Format* button on the Credentials tab that allows you to change the CHUID format of a Credential.
g. Shall support an *Auto Generate* button that allows you to randomly generate a PIN for PIN-only Credentials.
h. The SMS thin client shall provide a personnel image tab that includes image display, Image capture from a file or a local USB camera, and the capability to crop the Image and save it to the SMS personnel record.
i. The SMS thin client shall support the previewing/printing of badges.

5. The Thin Client shall support an Activity Monitor to provide a scrolling display of system activity. Activity shall be restricted based upon the Operator's Privilege and Partition assignments. Display controls shall include page up, page down, and a freeze function.

6. The Thin Client shall support acknowledgement of an Event from the Event Dynamic View.

7. The Thin Client shall support for logging an Event Message from the Event Dynamic View

8. The Thin Client shall support Manual Actions to include the Locking/unlocking of doors, and the Activation/deactivation of events.

9. The Thin Client shall support the display of Dynamic Views as defined by the SMS. Dynamic Views shall provide a real time view of SMS data including Journal and Audit Trail history. Viewing of Multiple Dynamic Views shall be supported.

10. The Thin Client shall support creating, configuring, loading and saving of reports. Reports shall consist of personnel history activity or audit data. The report data shall allow sorting within the thin Client view page by any displayed field in ascending or descending order. The Thin Client shall allow reports to be saved in the following formats: XLS, CSV, XML, TXT or PDF. The operator shall have the option to save the report to a file or send it via email.

11. The Thin Client shall support Manual Action Challenges. The Manual Action Challenge shall require an operator to enter their login credentials (User name and password) when executing a manual action, such as a door unlock, from within the Thin client.

12. The Thin Client shall support the ability to query on a specific cardholder or a group of cardholders for the purpose of assigning clearances to multiple cardholders at once. Once the query is complete, the operator shall have the ability to assign a single access clearance or a group of clearances to all cardholders.

13. The Thin Client shall support the ability to display a door activity report from the web client cardholder record configuration view. In addition, it shall provide the ability to display the Activation / Expiration Date and Time for each credential assigned to a cardholder. The thin client shall display all user-defined personnel fields and the details of each assigned access clearance in a separate window.

14. The Thin Client shall support Auto-Logoff based upon inactivity. The Thin Client shall monitor user activity and shall automatically log a user out of the workstation after a user defined timeout period.

15. The Thin Client shall support the ability to assign or remove clearances to multiple cardholders simultaneously.

2.3.G **SMS Mobile Application**

1. The SMS shall support a Mobile Application allowing operators to monitor or administer the SMS system by way of mobile device. The device shall be connected via the phone network and a VPN or via Wi-Fi to the SMS server utilizing Web Service (IIS - Web Service).

2. The SMS Mobile software shall be available for download from the following locations:
   a. Apple App Store
   b. Google Play

3. The Mobile Application shall support mobile phones and tablets running the following operating systems.
   a. Apple iOS 7.1 and higher (iPhone, iPad, iPod Touch)
   b. Android OS 6.0 and higher

4. The Mobile Application shall connect to a standalone SMS server, including an Enterprise Satellite Application Server (SAS) and Site Server (Appliance).

5. The SMS Mobile Application shall support connection to the SMS system through a 3G (minimum), 4G, or Wi-Fi connection.

6. The number of mobile connections allowed by the SMS server shall be based on the SMS licensing model. Each connection made through the SMS Web service shall be considered a simultaneous client connection.

7. Operator login to the SMS Mobile Application shall be consistent with the SMS thick client application, authenticating login credentials via Windows Single Sign-On (SSO).

8. The SMS Web Service shall require Internet Information Services (IIS) be installed on the target system. The SMS Web Service shall be installed on the IIS server during installation.

9. The SMS Mobile Application user interface shall be localized with supported SMS languages: Arabic, Czech, Danish, Dutch, English, French, German, Greek, Hungarian, Italian, Japanese, Korean, Polish, Portuguese (Brazilian), Russian, Simplified Chinese, Spanish, Swedish, Traditional Chinese, and Turkish.

10. The SMS Mobile Application shall support SSL-encrypted communications with the remote Mobile Web Service.

11. The SMS Mobile Application shall provide a search and filter option to refine query results.

12. The SMS Mobile Application shall provide a link to a context menu while viewing objects, providing the operator the ability to perform SMS operations consistent with the SMS administration and monitoring applications.

13. The SMS Mobile Application shall provide the following core features:
    a. The SMS Mobile Application shall provide operators with the appropriate privilege, access to tools used for inspecting the SMS Journal and Audit Logs.

    b. The SMS Mobile Application shall provide a collection of tools to monitor SMS events and other objects. Monitoring shall show active SMS events in real time.

    c. The SMS Mobile Application shall provide a collection of tools to manage personnel and shall allow for the following:

        i. Create/Update Personnel Records
        ii. Assign/Remove a card/credential to personnel.
        iii. Capture an image and associate that image with personnel.
        iv. Grace personnel, Antipassback Card Reset, Area Lockout Grace, and remove personnel from an Area.

    d. The SMS Mobile Application shall support the viewing of live and recorded video using American Dynamics VideoEdge NVR.

14. The SMS Mobile Application shall provide tools used to explore, edit and control the following objects:

    a. Favorite Filters
    b. Favorite Monitors
    c. Query
    d. Events
    e. Manual Actions
    f. Operators
    g. Controllers
    h. Doors
    i. Elevators
    j. Inputs
    k. iSTAR Clusters
    l. Outputs
    m. Readers

15. The SMS Mobile Application shall provide an editor for local application preferences such as:

    a. Login Parameters – Encryption, Inactivity Timer, etc.

b. Data Collection – Page Size
c. Monitoring – Polling Intervals, etc.

2.3.H **Graphic Maps**

1. The SMS shall support unlimited graphic maps and icons to be displayed on the operator workstation monitor.

2. The system shall support an operator-programmable, color graphic map display that:

   a. Shall be capable of showing the floor plan, the location of alarm devices, and alarm instructions for a facility.
   b. Shall be centralized in the system configuration and displayed on the operators' workstations.
   c. Shall allow various maps to be associated with different areas to create a hierarchy of maps.
   d. Shall support graphic maps having a resolution of 1024x768 Pixels or greater.

3. Operators shall be able to use drag-and-drop mouse technique to place dynamic system level object icons of all objects such as: cameras, video servers, inputs/outputs, events, maps, reports, dynamic views, and door/elevator icons. These dynamic object icons shall allow a system operator to perform tasks and issue commands related to the object by double-clicking on the icon.

4. The SMS shall allow the addition of new layers to the drawing (such that if the drawing must ever be reloaded due to an update of the drawing, the layer(s) created within the SMS will be added back automatically without additional reconfiguration).

5. The SMS shall be able to directly import the following file formats for the map:

   a. AutoCAD (.DWG)
   b. DXF
   c. JPEG (.JPG)
   d. PNG

6. The Maps feature shall include two operational modes: an administrative mode to allow configuring of the facility floor plans or site plans that show exterior features and a runtime mode to allow monitoring and interacting with the configured facility layouts or site plans.

2.3.I **Information Storage, Backup and Transfer**

1. All programmed information, as well as transactional history, shall be automatically stored in the database for later retrieval and backup. The SMS shall support configurations where the SMS database(s) may be installed on a hard drive on the SMS server, on an independent database server, or in an existing corporate database server.

2. The SMS shall be capable of backing up and restoring all system data and transactional history. The server shall be capable of transferring all programmed data and transactional history to CD-ROM, DVD, or Hard Drive (including networked drives).

3. The SMS shall allow activity history to be written to a database. The system shall have the capacity to store a minimum of 50 million transactions. There shall be a method of backing up the activity history on external media and then restoring and replaying it.

4. The SMS shall support AES 256-bit encrypted communications between server and user client.

5. The SMS shall support AES 256-bit encrypted communications between server and controller. The encryption shall support both local and third-party digital certificates.

2.3.J **Communication Ports**

1. The SMS shall be able to support multiple serial devices. In addition to COM1 and COM2, up to [8, 16, 32, to 256] additional ports may be configured through the use of a port expander or its equivalent. These serial ports may be used for connection to CCTV matrix switchers, or apC panels.

2. The SMS shall support the use of Ethernet networks as the communications path between the host computer and field devices such as, iSTAR, apC, apC 8/x, controllers, and CCTV matrix switchers. This communications path shall be the same network used for communications between the host server and the operator workstations. The communications between the host computer and the field devices shall be encapsulated in a TCP/IP network/transport layer. The SMS shall support IPv6. (IPv6 shall be supported only on C•CURE 9000 Clients and iSTAR Ultra controllers.)

2.3.K **Printers**

1. The SMS shall support report printing. The report printer(s) may be connected directly to the client PC, or shared over a network. The SMS shall support as report printer(s) any printer for which a printer driver exists within the Operating System supported by the current SMS version.

2.3.L **Software Configuration**

1. The SMS configuration tools shall utilize intelligent configuration controls. The system shall be structured so an operator is unable to perform configuration functions that are invalid based on the configuration used. The system shall support the ability to search within browser lists using filtering operators such as “begins with”, “ends with”, “contains”, etc. The system shall also allow an operator to do searches using filtering operators on any class of object in the system, both in the Administration application and the Monitoring Station application.

2. The SMS shall allow text description of all configured objects. The SMS shall allow the renaming of an existing title description without removing the sub-components of that configuration object. The SMS shall automatically remove from the system all configuration references to an object being deleted. The SMS shall automatically provide default names for all inputs, outputs, readers, and extension boards. The SMS shall clearly display which hardware objects (inputs, outputs, readers) on a controller are configured, and which are not.

3. The SMS shall provide for the configuration of templates. Templates of supported objects shall be operator-configurable to provide default values by pre-populating commonly used data fields.

4. The SMS shall support an unlimited number of groups for any object type. The SMS shall support unlimited object group definitions. In general, a group shall be usable wherever an individual object is referenced in the SMS. For example, a group may be used instead of an object when configuring a schedule/object pair in a clearance, and a group may be used instead of an object when performing a manual action to unlock a door.

5. The SMS shall generally allow any object in the system to be grouped including personnel, doors, inputs, outputs and clearances.

5. The SMS shall restrict the viewing and controlling of objects in the administration and monitoring stations via operator privileges. The SMS shall support the configuration of operator restrictions on an object class basis, and on an object-by-object basis. The SMS shall maintain a distinction between objects that are being monitored and objects that are being controlled, preventing operators from issuing object manual actions to objects for which the operator does not have manual action privileges. There shall be different levels of controls within the system for administration privileges versus monitoring privileges.

6. The SMS shall support unlimited operator accounts with unlimited definable privilege levels.

7. The SMS shall allow configuration of controllers using hierarchical tree-based navigation and context menus.

8. The SMS shall support the ability to download firmware updates to the controllers.

9. The SMS shall support the following methods for Operator authentication and authorization:

    a) Windows Single Sign-On (SSO).

    b) Basic User Authentication with locally defined user names and passwords with strong password rule enforcement.

10. The SMS shall provide an automatic client update process for quick distribution of application updates.

11. The SMS shall have context sensitive online help (at the screen level) available at any point requiring operator input.

2.3.M **Workstation Support**

1. The SMS shall support a Workstation Dynamic View which shall list at a minimum:
   a. The Workstation Name
   b. A Description
   c. Enabled/Disabled status
   d. Last known Operator

2. Last known Application/connection type with version information

3. The SMS shall support the ability to disable any Workstation preventing any Operator Login from disabled Workstations.

2.3.N **User-Defined Fields**

1. The SMS shall support an unlimited number of User-defined fields. Each user-defined field shall allow a name, description and a customizable label. A default language shall be selectable by the System Administrator for the user-defined field labels.

2. User-defined fields shall support customizable character size restrictions which shall limit the size of the field.

3. User-defined fields shall be usable for reports, queries, dynamic views and exports of system data.

4. User-defined fields shall be available for the following SMS objects:

   a. Personnel
   b. Credentials
   c. Field Controllers
   d. Inputs
   e. Outputs
   f. Events
   g. Card Readers
   h. Doors
   i. Elevators
   j. Clearances
   k. Visits
   l. Access Requests
   m. Video Cameras/Servers
   n. CCTV Switches/Cameras

5. User-defined fields shall be definable as Mandatory and/or Unique and shall support the following field types:

   a. Character

b. Integer
c. Logical
d. Date/Time
e. Date
f. Time
g. Enumerated List
h. Multi Line
i. Decimal
j. Identity

6. User-defined fields shall support masking to provide consistency of data entry across all system operators. Custom masks, as well as the following predefined masks, shall be available:

   a. Alphabetic
   b. Alphanumeric
   c. Numeric
   d. Phone Number – USA
   e. Zip Code
   f. Zip Code +4
   g. Alpha – All Caps
   h. Alpha – All Lower case

2.3.O **Personnel Records**

1. The SMS shall provide Personnel Templates that shall eliminate repetitive data entry by pre-configuring Personnel Records with data common to all Personnel of a certain type.

   The SMS Personnel records shall provide multiple tabbed pages of personnel data containing default system and user-defined fields. Labels for user-defined field tabs shall be customizable by the System Administrator with the appropriate privileges. The SMS Personnel record shall support the creation of tabs allowing for additional user-defined fields.

2. The SMS shall support a Watchlist flag for all Personnel to identify individuals requiring special attention.
3. The SMS shall provide assistance alerts in the form of a button on the Personnel screen for the operator to request assistance from another operator via an event activation.
4. The SMS shall provide a “Personnel Record Document Object” option which allows the operator to assign / attach up to two (2) documents (such as URL, PDF, or TXT files) to the personnel record. The document may be applied to the record as a:

   a. 'Shared' Document - added to the SMS via the Documents Editor.
   b. 'Private' Document - imported from outside the system, such as a birth certificate or a diploma.

5. The SMS shall include a "Documents" tab to user-defined personnel views as well as the default view "*Personnel View with Portrait in Header*" to support the association of

documents. The documents are available for viewing by operators with appropriate privilege.

6. The SMS shall support the generation of a unique random card number for an access credential for all Personnel records. The unique card number shall contain up to the maximum number of digits for the CHUID format chosen for the credential.

7. The SMS shall support the configuration of a trigger for a Personnel record that pulses an Event whenever a 'Card Admitted'/'Card Rejected' message is logged to the Journal for that person at a defined Door/Elevator.

8. The SMS shall support an email address field for each Personnel Record and shall support the sending of emails to Personnel Groups.

2.3.P **Credentials**

1. The SMS shall support a minimum of five (5) credentials (cards) per Personnel record and shall only count Active and/or Expired Cards towards the maximum assignable Cards per Person. Cards designated as Lost, Stolen and Disabled shall not count towards the maximum assignable Cards per Person.

2. The SMS shall support the ability to define the default period of time (in Days, Hours or Years) from a Credential's Activation Date until its Expiration. The SMS shall support an override of the default Expiration time period for individual Personnel Types.

3. The SMS shall support Temporary Credentials. Temporary Credentials shall be available for general re-use without being associated to specific Personnel records. Temporary Credentials shall be assignable to visitors and can also serve as temporary replacement cards for Personnel who misplaced or forgot their regular Credentials. The SMS shall support the configuration of a default number of days for Temporary Credentials to remain active after they are created.

4. The SMS shall provide the ability to define background colors for the Active/Expired Credential Status fields in the Personnel Record.

5. The SMS shall support a system-wide setting to automatically disable Personnel Credentials that have not been used for a specified period of time. The Disable by Inactivity process shall support a user configurable daily scan time.

2.3.Q **Personnel Views**

1. The SMS shall support user-defined Personnel Views. Personnel Views shall provide the ability to customize the Personnel record by adding and/or removing certain objects from the operator's view. Personnel Views shall be assignable to SMS operators via the operator's assigned privilege and shall be definable for use in the creation and/or editing of the Personnel record. All Personnel Views enabled for an operator shall be selectable from the current view to allow an operator to switch views in real time. Personnel Views shall support the following:

a. Adding/Removing Fields (including all user-defined fields)
b. Custom Field Labels
c. Adding Boxes to group together common fields
d. Adding/Removing tabs to organize fields
e. Custom Tab Labels
f. Customization of Tab display order
g. Background/Foreground color control of fields and labels
h. Personnel Record Document Object – to associate up to two (2) documents to the record

2.3.R **Language Localization**

1. The SMS shall be configured so the information presented to system operators is displayed in a language native to the system operator provided that the proper translation files exist.

2. It shall be possible to translate the SMS into any left-to-right or right-to-left language supported by Unicode and by the Microsoft Windows operating system.

3. Languages shall include English, Arabic, Brazilian Portuguese, Czech, Dutch, Danish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Polish, Russian, Swedish, Simplified Chinese, Spanish, Traditional Chinese and Turkish. .

2.3.S **Inputs**

1. The SMS shall monitor both supervised and unsupervised hardware inputs as well as virtual inputs such as predefined system messages. These inputs include door / elevator inputs and monitor points. The SMS shall also monitor controller inputs such as tamper, AC fail, and low battery.

2. The SMS shall have the ability to name and allow for user-defined descriptions for individual inputs, outputs, and readers as well as input and output modules.

3. There shall be three separate and distinct states for inputs, which can be defined on the input configuration screen: Disabled, Enabled / Disarmed and Enabled / Armed.

4. The SMS shall allow configuration to link the state of an input to an output. The system shall allow multiple inputs to activate a single output or group of outputs.

2.3.T **Outputs**

1. The SMS shall have outputs, also known as Control points, which associate an input or event action with a relay output. These output uses include doors / elevators, alarms and industrial control.

   There shall be three types of outputs available: dry contact / Form C relays, wet or voltage sourced relays and Open Collectors. Outputs shall be configured such that they can be activated, deactivated or pulsed by system actions.

2.3.U **Card and Reader Support**

1. The SMS shall be designed to support multiple card formats and card reader types.

2. The SMS shall support the following features for directly connected readers:

    a. OSDP. (Open Supervised Device Protocol), v2.1.6 or higher. OSDP shall only be supported with the iSTAR Ultra and qualified OSDP capable readers using OSDP Secure Channel AES128 encryption.
    b. User definable options pertaining to LED and Beeper control.
    c. User defined card formats up to 256 bits.
    d. Unlimited number of SMS card formats.
    e. The ability to assign up to 10 card formats per reader.
    f. The ability to show reader status on RM LCD.
    g. Support Wiegand and 3x4 matrix keypads.
    h. The enrollment of biometric templates to smartcards.
    i. Custom CHUID FIPS201-compliant supporting full 256-bit data.
    j. The SMS shall support readers that provide Wiegand signaling and magnetic signaling to include:
        i. Software House RM readers.
        ii. Software House Multi-technology readers.
        iii. Wiegand swipe/insert readers.
        iv. Proximity readers.
        v. Biometric readers.
        vi. Smart card readers.
        vii. Wireless readers.
        viii. Magnetic readers.

2.3.V **CCTV Integration / Digital Video**

1. The University of Utah utilizes Avigilon ACC VMS Software campus Wide. The SMS shall provide extensive integration with the Avigilon Video Management System.

2.4 EQUIPMENT

2.4.A iSTAR Ultra Access Control Panels – Model USTAR016

1. **University Standards require iSTAR Ultra Panel USTAR016 in a hardwired configuration only with all readers and field devices home run to central location using composite access control cable (Part Number XXX-XXX). Provide 20% spare capacity on all panels to support future growth. The use of RM-4 door modules and wireless locksets is expressly prohibited unless specified and approved by the University.**

    Any inputs or outputs not associated with a card reader door will require the addition of I8 or R8 remote input/output modules to the panel to support the

additional I/O requirements. These inputs and outputs may include but not be limited to, panic and lockdown switches, elevator controls, fire alarm inputs, door contacts, intrusion detectors, call buttons or other monitoring/control systems.

Independent of conduit, conduit systems or wire tray, each iSTAR Panel and Dual Voltage Power System will require 4x4 gutter for wire management which is the responsibility of security installation contractor.

2. iSTAR Ultra is a powerful, network-ready controller that supports up to 32 readers. The strong feature set answers the most demanding access control requirements of enterprise and government applications. Rack-mount and wall-mount options provide installation flexibility, while iSTAR Ultra's unique lock power management eliminates the need for separate lock power interface boards. iSTAR Ultra features a hardened Linux kernel for its operating system, improving the security and scalability of the system.

3. iSTAR Ultra uniquely combines support for traditional hard-wired access control doors with support for wireless lock sets, all in the same controller. Up to 32 readers are supported by the iSTAR Ultra, of which 16 may come from the Access Control Module's (ACM) I/O units – the rest can be made up of wireless lock sets and devices.

4. iSTAR Ultra is ideal for areas that require many readers in close proximity to the panel. For more distributed installations, iSTAR Ultra includes up to 16 RS-485 ports, allowing the installer to run longer distances to each door.

5. iSTAR Ultra uses a General Controller Module (GCM) which includes standard 2GB RAM and 16GB SD card for memory, and has two onboard gigabit network ports for reliable network communications. The GCM controls up to two ACMs, with each ACM supporting up to eight Wiegand or RM readers, along with 24 supervised inputs and 16 outputs which can be individually wet- or dry-configured.

6. iSTAR Ultra also includes an alphanumeric LCD to provide status and troubleshooting information. Database backups and all buffered transactions are stored to non-volatile SD card memory. A real-time clock battery keeps the clock powered during a power failure.

7. iSTAR Ultra includes two onboard gigabit network ports for primary and secondary communications to the host. 256-bit FIPS 197 and FIPS 140-2 AES network encryption, with custom key management, secures the controller from potential network threats. iSTAR Ultra supports both static and dynamic IP addresses, using DHCP and DNS to simplify network installation. In addition, the powerful iSTAR Configuration Utility (ICU) reduces startup time by allowing you to view online controllers, change configuration parameters, and download new firmware from a single interface.

8. Embedded Lock Power Management. The iSTAR Ultra's ACM offers a unique, straightforward approach to managing the complete lock power needs of an

installation. The ACM is designed to distribute power directly to each lock circuit without needing a separate fused distribution board (and the associated interconnect wiring). Each ACM has two separate lock power feeds in addition to controller power.

9. These feeds can be used for different voltages (12 V and 24 V for example) or for battery-backed and non battery-backed power sources to comply with certain local life safety codes.

10. Each lock output can then be selected to use either a dry contact, lock power 1, or lock power 2, providing tremendous flexibility. In addition, each lock circuit is protected with a PTC resettable fuse and over-voltage surge protection through the extensive use of transzorbs, and includes a socketed relay for quick field replacement. Each lock circuit can be individually selected to unlock or lock based on the dedicated fire alarm input setting, meeting life safety requirements.

11. Ensure Reliable Communication with Clusters

12. iSTAR Ultra supports peer-to-peer communications across clusters meaning that the controllers communicate with one another without needing host intervention. Clusters are user-defined groups of up to 16 controllers and can be created to enhance security by separating a widely dispersed facility into different controlled areas. For example, events linking inputs on one controller to outputs on another controller will still be active without the host.

    a. Powerful network-ready door controller for up to 32 readers (16 from ACMs)
    b. Embedded lock power management lowers installation costs
    c. Hardened Linux embedded OS for improved security and scalability
    d. Includes global anti-passback and advanced peer-to-peer clustering
    e. Native intrusion zone functionality • LCD provides important controller status and diagnostics information
    f. Manages up to 500,000 cardholders in local memory
    g. Dedicated input for fire alarm interlock overrides door locks during fire conditions
    h. Onboard 256-bit AES network encryption
    i. Tested and validated for FIPS 140-2 under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program
    j. Compatible with C•CURE 9000 v2.30 and above2
    k. Enables ASSA ABLOY Aperio or Schlage AD300 and AD400 wireless locks to communicate with C•CURE 9000 providing a fully integrated and managed lock solution
    l. Rack-mount models provide flexibility in mounting options
    m. Great solution for enterprise and government installations

2.4.B PSX Dual Voltage Power Systems – Model PSX-ISU-E2

1. PSX Power Solutions Dual Voltage Power System PSX Dual Voltage Power System is a high efficiency, offline switch mode, dual voltage power supply battery charger designed to provide both iSTAR Ultra system power, and lock power for a complete 16-door setup. Capable of providing multiple power outputs and featuring user select ability for 12 or 24V DC on the lock supply, the wall mount unit is configured in a painted steel, locking enclosure with tamper switch and integral battery space. The rackmount unit is configured in a 2U rack enclosure.

2. One power supply (150W) in the PSX Dual Voltage Power System connects directly to the main power input of the iSTAR Ultra (GCM and ACM boards). The second power supply (250W) connects to the dedicated lock power inputs on the ACM boards, providing an efficient method to manage power to each separate locking device. PSX Dual Voltage Power System offers optional fire alarm interface (FAI) control for power and control of locks, and other devices.

3. PSX Dual Voltage Power System provides fault relay outputs for connection to inputs on the iSTAR Ultra. One relay output is connected to the power fail input and indicates loss of AC power to the PSX Dual Voltage Power System. The second relay output is connected to the low battery or fault input, and indicates low battery or a problem within the power supply. The relays from both power supply units may be interconnected, if desired.

4. The unit is equipped with LED indicators which indicate current status. The unit will accept an optional remote management device providing remote monitoring, remote battery testing, along with many other capabilities. A network monitoring module is available as an option. The PSX Network Communication Board provides the PSX Dual Voltage Power System with the ability to offer remote monitoring and control over LAN/WAN.

5. With the optional PSX Power Solutions Network Communication Module, power supplies, battery condition, fault status, and temperature may be monitored and configured for remote notification via email or SNMP. Remote battery testing of either battery set may be implemented manually or on a scheduled basis.

    a. Provides uninterrupted back-up power for a complete iSTAR Ultra, 16-door setup, including locks
    b. Choice of wall mount and rackmount models
    c. Supervision of AC fault, system fault, ground fault, reverse battery, and fire alarm activation
    d. Switched and resettable outputs
    e. Network communication interface option
    f. Intelligent battery charging and battery state monitoring
    g. Dual rate charging restores battery sets from 4Ah to 80Ah
    h. Reverse polarity, overcurrent, and thermal overload protection
    i. Wall mount: 4.5” enclosure depth accommodates 12Ah battery sets
    j. Rackmount: Enhanced input and output surge suppression
    k. RoHS compliant, lead free, high efficiency designs

l. UL603 and UL 294 compliant
m. Lifetime warranty

2.4.C Software House I8 & R8 Remote Modules

1. The Software House I8, R8, and I8-CSI modules provide a flexible, cost-effective means to expand the input and output functionality of any iSTAR or apC access controller. Common applications include alarm monitoring and control and elevator control.

2. The I8 input module provides eight Class A supervised inputs. Three LEDs per input help the installer commission and troubleshoot each input circuit – red if the input is in alarm, green for normal, and yellow for a supervision error. LEDs may be turned off via a DIP switch setting. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

3. The I8-CSI module enhances the functionality of the standard I8 module by supporting numerous supervised circuit types and EOL resistance values. This allows the I8-CSI to accommodate existing field wiring without changing EOL resistors. More than 20 different circuit types are supported. The circuit type is selected via a bank of DIP switches and applies to all eight inputs on the I8-CSI.

4. The R8 output module provides eight Form C dry contact relay outputs. A red status LED per output shows the state of the relay.

5. All modules feature a dedicated input for an external cabinet tamper switch and mount easily in the Software House RM-CAN or RM-DCM-CAN enclosure.

6. The modules communicate with iSTAR or apC controllers via the two-wire RM bus that allows total wiring distances of up to 1,220 m (4,000 ft).

7. Up to eight I8s and eight R8s can be connected to each apC, iSTAR eX, and iSTAR Pro eight-reader model; up to 16 of each module can be connected to the iSTAR Pro 16-reader model. The modules are fully compatible with both C•CURE 800/8000 and C•CURE 9000.

a. Provides cost-effective expansion of input and output capacity
b. Compatible with full range of Software House iSTAR and apC access control panels
c. Locate modules up to 1,220 m (4,000 ft) away from controllers using flexible two wire RS-485 RM bus
d. Reduces length of sensor and control wiring to save installation costs
e. I8 provides eight Class A supervised inputs
f. R8 provides eight Form C relay outputs
g. I8-CSI, configurable supervised input model, allows use of existing input wiring without changing end-of-line (EOL) resistors
h. Three status LEDs per input (red/yellow/green) and one per output enable quick diagnostics and troubleshooting
i. Small, modular size requires minimal panel space
j. Dedicated tamper input included on each module

k. Optional UL-listed enclosure available

2.4.D Composite Cable for Card Reader Doors – ACCESSJKTPLEN 18-4C

1. Product Description: FRPVC Bare copper conductor 4-component composite cable; each component is shielded and jacketed. Diameters and weights may vary among manufacturers. Flouropolymer jacket.

   Sheilded

   a. Component 1: 18-4 C Lock Power
   b. Component 2: 22-2C Door Contact
   c. Component 3: 22-4C Rex Spare
   d. Component 4: 22-3P Card Reader

2. UL Listed Type CMP For use in security access control systems.

3. Specifications ACCESSJKTPLEN 18-4C 22-2C 22-4C 22-3P 0.435 126

   a. CONDUCTOR: Bare copper, stranded A325
   b. INSULATION: Flame-retardant polyvinyl chloride (FRPVC)
   c. SHIELD: Aluminum/Mylar with tinned copper drain wire (each component is shielded)
   d. OVERALL JACKET: Yellow flame-retardant plenum jacket
   e. STANDARDS: NEC: CMP, NEC Article(s) 800
   f. RATINGS: 75°C, 300 VUnshielded

2.4.E Card Readers

1. **HID Global - R40 (920NTNNKO) for Standard Applications, R15 (910NTNNKO) for Mullion Mount Applications, RK40- (921NTNNKO) Where specified for PIN + Card Applications and the Software House TST-100 Touchscreen Terminal for High Security with Arm/Disarm locations as Specified.**

2. Provide HID Global iClass SE Readers with layered security beyond the card media for added protection to identity data using SIOs. Interoperable with a range of technologies and form factors including mobile devices utilizing Seos. Capable of Open Supervised Device Protocol (OSDP) for secure, bidirectional communication and for advanced security, the readers utilize state-of the-art authentication through the platform's Secure Identity Object (SIO) data model for trusted and secure communication between the card and reader to prevent unauthorized access. The iCLASS SE reader line is built on the Security Industry Association (SIA) Open Supervised Device Protocol (OSDP) standard which also ensures secure transmission of data from the reader to the controller.

   a. iCLASS SE® Readers can be easily and securely managed in-field through the HID Reader Manager Mobile App. With the addition of our Bluetooth Smart Module or Bluetooth Smart/OSDP upgrade kit, you can update firmware, LED color, beeper

response and credential keys or upgrade existing readers to support HID Mobile Access®.

b. Multi-Layered Security – Ensures data authenticity and privacy through the multi-layered security of HID's SIO.
c. EAL5+ Certified Secure Element Hardware – Provides tamper-proof protection of keys/cryptographic operations.
d. Secured communications using OSDP with Secure Channel Protocol.
e. Expanded iCLASS Elite™ Program – Extends private security by protecting uniquely keyed credentials, SIOs and programming keys.
f. Intelligent Power Management (IPM) – Reduces reader power consumption by as much as 75% compared to standard operating mode.
g. Industry standard communications using OSDP.
h. Custom programming support to read models on MIFARE and MIFARE DESFire EV1 credentials

2.4.F Software House TST-100 Touchscreen Terminal

1. The SWH TST-100 touchscreen terminal connects securely over full duplex RS-485 to an IP-ACM Ethernet Door Module using AES 256 encrypted communication. Multi-Tech Read Head Offers Flexibility, the TST-100 Touchscreen Terminal

2. simultaneously supports MIFARE, DESFire EV1 and EV2, HID iCLASS, iCLASS SE, iCLASS Seos, and HID Proximity card technologies. This allows customers to transition from a proximity system to a more advanced smart card system, or to maintain an existing universe of proximity cards while gradually moving to smart card technology.

3. The read head supports PACS data from HID iCLASS, iCLASS SE, and iCLASS Seos smart cards. Performance can be optimized by prioritizing and disabling card technologies through a local setup mode. A simple firmware download ensures that the read head is kept up-to-date with the latest fixes and enhancements.

4. "RM Mode" Provides Compatibility when connected to an IP-ACM Ethernet Door module, the TST-100 Touchscreen Terminal operates in "Smart Mode," providing the full icon-driven interface. The reader also supports the legacy RM protocol, allowing it to connect directly to any iSTAR door controller and operate as if it is a standard RM reader, providing a great upgrade path.

5. Future-Proof Solution The TST-100 Touchscreen Terminal is more than a reader – it provides a powerful platform for future applications and use cases. An embedded speaker and microphone are built in, ready to be supported through our future intercom application. Future apps will be supported through a simple firmware update.

2.4.G Request to Exit Motion Detector – Model DS160

1. Provide Bosch DS-160 Series High performance Request to exit Detectors specifically designed for Request-to-exit (REX) applications. Motion Detector will include features

such as timers, door monitor with sounder alert, and point able coverage, the DS160 and DS161 have the flexibility to meet the most stringent REX requirements. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

2. The exclusive Sequential Logic Input (SLI) provides added security by allowing connection of a second device to require sequential detection. This eliminates the possibility that an object that is slid through the door or underneath the door will activate the detector. This input can also be used to lock the sensor if motion is present outside the premises. University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.

    a. Door Monitor sensor can monitor a door contact to allow special control of the internal relay. For example, if the door is opened within the relay time period, the sensor can be programmed to halt the timer. If the door is not opened within a specific time period, the relay can be programmed to deactivate.
    b. Sounder Alert An integrated sounder can be programmed to activate if the door is left open too long. The sounder volume is fully adjustable to 85 dB.
    c. Keycard Input The keycard input allows the sensor relay to be controlled from an external source, such as an access control system or card reader.

2.4.H Request to Exit Push Buttons and Key switch Overrides

1. University Standards require on all doors with Electromagnetic Door Locks or that require secure or delayed exit as per occupancy requirements, provide a Camden CM-30EE 2” Illuminated Green Exit Push Button with Electronic Timer on exit side of door and a Camden SPDT Maintained Key switch Override on the secure side of the door. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

2. **REX Push Buttons:** Camden CM-30EE illuminated exit switches are high visibility 'request to exit' (REX) buttons, backlit in green with black PUSH TO EXIT text. They are supplied with a single gang industrial grade stainless steel faceplate and tamperproof screws.CM-30EE is supplied with an integrated 30 second fixed timer. CM-30AT is supplied with an adjustable 30 second timer. Pushing the button cuts power to the magnetic lock and activates the timer.

3. **Key switch Override:** Camden Key switch Override CM-1130 SPDT Maintained Key Switch Override fits standard single gang boxes, 1 piece die cast construction, Locators prevent cylinder from spinning, Vandal resistant Cylinder sits flush to faceplate, Indoor or outdoor applications, Left and/or right operation, Color coded 18 AWG soldered leads, Heat shrink protective sleeve over contacts, Casted center rib protects switches from damage, SPDT maintained.

2.4.I Door Position Switches – Pedestrian Doors

1. Provide George Risk Industries (GRI) 180 Series ¾” or 1” Steel Door Recessed Door Switches. The GRI 180 Series is the industry standard 3/4" diameter recessed steel door switch set with 12” Leads and the the 184 Series is a 1" diameter switch set. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

    a. Lifetime Warranty
    b. Colors: White, Brown, Grey or Black
    c. UL and ULC Approved
    d. 180-12 & 184-12 UL 10C Fire Rated
    e. Available in Closed Loop, Open Loop and SPDT
    f. 3/4" and 1" Diameter Mounting
    g. Standard 12" Leads or Terminals
    h. Self-Locking
    i. Solid, One Piece Design
    j. 7/8" Diameter also Available - Call Factory
    k. Switches or Magnets are Available Separately
    l. Standard 1/2"+ Gap on Steel
    m. Wide Gap 1"+ Gap on Steel
    n. Supervisory Loops Available

2.4.J Door Position Switches – Overhead Doors

1. All Overhead Doors require Potter Electric ODC-59 Series Overhead Door Contacts with a 2” Operating Gap which are exclusively designed for rugged high traffic installations. The reed switch is hermetically sealed with a PVC shock absorber enclosed within a solid aluminum housing. Installation wires are protected in a 24" stainless steel armored cable. The ODC-59 Series magnet is mounted on an adjustable L shaped bracket designed for greater flexibility, universal mounting, greater pulling power, and to provide a professional installation appearance. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

2.4.K Building Lockdown Switch – Sentrol 3040

1. The 3040 Series Panic Switch activates the SPDT switch (SPST on the 3045 model) when the user pulls the actuating lever. On the 3040 model, an external LED lights and latches, indicating that the alarm circuit has been activated. The lever is closed first to rearm the alarm switch, then the latching LED circuit is reset externally at the host panel. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

2. The unit consists of a housing that contains the electrical circuitry and magnetic reed contacts, a cover plate to protect the internal electronics and an actuating lever with an Alnico V magnet installed in a cradle in the lever. When the lever is fully closed, the magnet — in proximity to the reed —triggers the circuit. The alarm occurs when the actuating lever is moved 20° to 45° past the fully closed position (approximately 1" from the fully closed position). On the latching models, an LED on the unit flashes and latches when the lever is

opened. It can be reset only at the alarm panel. The actuating lever, housing and cover plate are made of ABS fire-retardant plastic. Dimensions of the unit are 1.77"W x 2.90" L x 0.76" H (4.50 cm W x 7.37 cm L x 1.93 cmH). The unit has 12 feet of jacket lead. The device mounts to the surface with two No. 6 combo-head screws, 5/8" and1 1/4". Available in white

2.4.L Panic Alarm – Amseco/Potter HUSK20

1. The HUSK-20 is a mechanical hold-up switch designed for silent operation. It is activated by using one finger to press down on the switch. When activated, the switch mechanism locks, insuring an immediate alarm signal. A status window designed on top of the hold-up switch indicates its condition: RED (alarmed) and BLUE (armed). To reset the HUSK-20, use the key provided. The housing is made of metal and is painted gray. **University Standards require that all inputs on the system require true 2 resistor end of line supervision with (2) - 1K 1/8 watt 5% carbon film resistors.**

2. The hold-up switch sends a signal to a dedicated 24 hour hold-up circuit of the access control system. That signal in turn will send the immediate signal to police or central station.

    a. Form C contact
    b. Metal housing
    c. Key reset
    d. Silent operation
    e. Status window indicator (armed, alarmed)
    f. Mechanical operation
    g. Terminals for easy wiring