Standards for Electronic Security Systems

April 14, 2016
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.O.C.</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>2</td>
</tr>
<tr>
<td>Security Management Description</td>
<td>3</td>
</tr>
<tr>
<td>Design Standards</td>
<td>5</td>
</tr>
<tr>
<td>Implementation Guidelines</td>
<td>14</td>
</tr>
</tbody>
</table>
Background

The purpose of this Security Standard Document is to document the specific goals and objectives of the Security Management System for the University of California, Davis (UCD), to define the major system software and hardware components that comprise the SMS, and to provide general the design guidelines for integration of the SMS into new and existing building projects and site improvement projects throughout UCD facilities. The principal goal of this document is to provide consistent design and implementation standards for the integration of physical electronic security devices. The design standards included in this document describe system device performance requirements for each of the applicable devices that may be included within a specific project. The subsequent implementation standards establish a protocol for device type selection – when and where to install a particular devices.

Historically, the implementation of security systems and infrastructure in new and retrofit building projects at UCD has been determined by various entities that have are not directly responsible for the safety and security of the students, staff and facility. This resulted in fragmented group of systems that are unmanageable for UCD Police. Recently, UCD has undertaken the incorporation of all Building Intrusion Alarms Systems (BIAS) into a centralized monitoring and control platform that now allows alarms throughout UCD facilities to report directly to Campus Police Dispatch. This has improved response times to alarms and increased the reliability and functionality of these systems. UCD Police have set a goal to centralize monitoring and control of the Access Control Systems and Video Surveillance Systems that are deployed throughout the Campus and facilities. Achieving this goal is more complex than the centralization of the BIAS but it is not insurmountable. The initial step in the process was to establish and implement a Security Management System that serves as the nexus for Campus wide control and management of access controlled doors and video surveillance cameras.

The Security Management System (SMS) is a unified security management platform that provides integration capabilities for four primary security sub-systems. The purpose of this implementation standard is to document the specific goal and objectives of the SMS, to define the major system software and hardware components that comprise the SMS, and to provide general design guidelines for integration of the SMS into new and existing building and site improvement projects on Campus.
The Security Management System is a unified security management tool that provides UCD Police with a physical security information and situational awareness management system. The SMS serves as a foundational tool used by UCD Police in their continuing efforts to ensure a safe and secure learning environment for students, faculty and staff.

The SMS is comprised of three major electronic security sub-systems.

- Access Control System (ACS)
- Building Intrusion Alarm Systems (BIAS)
- Video Surveillance System (VSS)

Each of these sub-systems is comprised of command/control hardware and software and field devices. The command/control hardware and software are standardized so as to provide UCD with a single, unified operational platform for the physical security systems management. Security field devices will be designed and specified on a project specific basis throughout the course of the execution of new and retrofit construction. Individual projects may include hardware and software components (i.e. data storage and licenses) that are added to increase the capacity of the UCD system/sub-system. Not all of the devices described in this document will necessarily be included in each project. It is the responsibility of the design team assigned to each project to use the security standards and protocols in this document to develop the appropriate deployment strategy and device requirements for their particular project.

**Access Control System**

The ACS is the core platform of the SMS. It is a software based system that provides the command and control functionality for the access control doors and associated alarm devices, stores access control credentials and privileges (ID Cards), provides the primary graphical user interface for monitoring and managing electronic security events and alarms, and serves as the central repository for system events that can be used for investigative and administrative purposes. In addition, the SMS provides the central integration facilities for the other electronic security sub-systems through seamless system software interoperability and management that provides a single human-to-system graphical user interface for the configuration, management and control of these systems.
**Building Intrusion Alarm System**

The BIAS is primarily hardware based. It is comprised of existing building and room alarm panels and associated field devices. These systems are identical to small commercial and residential “burglar alarm systems” in that the panel receives alarm signals from various field devices and, when the system is armed, transmits that alarm information to a central alarm monitoring system. The centralization of the BIAS is largely complete at UCD and the integration of the BIAS into the SMS will provide UCD Police with centralized, integrated alarm interface that ties graphical mapping capabilities and real-time and recorded video into the existing alarm monitoring capabilities.

**Video Surveillance System**

The VSS is a software based sub-system that operates at a deep integration level with the SMS. The software provides configuration, control, monitoring and recording management of digital video cameras and digitally encoded signals from analog cameras. By being a fully integrated component with the SMS, video monitoring is an event based practice where specific video data is displayed when associated with a particular programmed alarm event within the system. This feature serves as an effective situational management tool for UCD Police to utilize on a real-time basis. In addition, all cameras are recorded within the system and video is to be stored for a minimum of 30 days so the VSS also serves as a valuable investigative tool. The system is network based and is substantially reliant on the network backbone infrastructure for transmission of video data. VSS recording devices, which have a substantial amount of drive space allocated for storage, are distributed throughout buildings and facilities to reduce network traffic demand and to provide fault tolerance.
Design Standards

This section includes technical standards data and criteria that should be used, in whole or in part, by security design professionals on a project specific basis. The intent of the material provided is to serve a guideline for establishing performance criteria and maintaining conformance UCD Security System Standards. The systems designed on particular projects must maintain conformity and operation with the SMS software as described and installed. As such, major system components are manufacturer specific and substitution will not be permitted. However, field devices are specified on a performance basis. Where make and models are specified, the information is to serve solely to establish performance criteria. In such cases, make and model information will be followed by, “or equal” and should be specified as such in the project specific design documentation.

General Security Requirements

A  CODES AND STANDARDS
All work shall be in accordance, where applicable, with the latest edition of the following:

- California Building Code – Title 24 (CBC)
- California Electrical Code (CEC)
- California Fire Code (CFC)
- Electronics Industries Association (EIA)
- Institute of Electrical and Electronic Engineers (IEEE)
- National Electrical Manufactures Association (NEMA)
- Occupational Safety and Health Act (OSHA)
- All other State and local codes and ordinances that may prevail

B  DESCRIPTION OF WORK
Work includes the design, procurement and installation of SMS devices and equipment and integration of the devices and equipment to UCD’s SMS, comprised of the following sub-systems:

- ACS
- BIAS
- VSS
Specific devices types, locations and interconnection requirements are described and detailed within project specific documents, in accordance with these UCD Security Standards.

Security related work may require system configuration and programming of existing UCD systems. Coordinate all such configuration and programming requirements with the UCD.

C QUALIFICATIONS OF CONTRACTOR
The Contractor should maintain all current licenses required to provide the specific work efforts of the specific project.

The Contractor should utilize installation and service technicians whom are competent; factory trained and certified personnel capable of installing and maintaining the system and providing reasonable service.

D MATERIAL SUBSTITUTIONS
Whenever materials, equipment or processes are specified or described in this Standard by using the proprietary name of an item or the name of a particular manufacturer, fabricator, supplier or distributor, the naming of the item is intended to establish the type, function and standard of quality and performance required by this Contract. It is not the intent of UCD to exclude other materials, equipment, or processes or to limit competition in bidding. Therefore, unless the proprietary name referred to in the specifications is followed by words indicating that no substitution is permitted, materials, equipment, or processes of other manufacturers, fabricators, suppliers, or distributors will be considered by UCD for substitution.

Consideration will be given to a proposed substitute only when sufficient information is submitted to UCD to determine that the proposed substitute material, equipment, or process is in fact equivalent in all respects to the materials, equipment, or processes named in the specifications.

Where the phrase “or equal,” occurs in this Standard, do not assume that the materials, or equipment, will be approved as equal until the item has been specifically so approved for this work by UCD.

The Owner, based upon conformance and integration with existing system equipment, has selected primary system components as specified. No substitutions will be accepted for these components.
E INSTALLATION
Systems, equipment and devices should be installed by competent tradesmen, skilled in this class of installation.

Systems should be installed in a manner that is consistent with the provisions and intent of the project specific Specifications, the Drawings, and the referenced Codes and Standards, and in accordance with equipment manufacturers’ written Specifications and instructions and these Standards.

Installation workmanship should be accomplished in a neat and professional manner, meeting industry standards.

F ACCEPTANCE TESTING AND COMMISSIONING
On-site Acceptance Testing with witness by UCD, providing all personnel and equipment necessary to perform these tests, should be included in each project referencing work included in this standard.

Acceptance Testing should include operational verification and testing of all new and existing devices installed, modified and/or associated with the scope of this Project.

Security Management System Requirements
A SMS SERVER AND SOFTWARE
The SMS server is existing. It resides on the UCD Ethernet infrastructure on a dedicated security VLAN. All ACS panels and devices specified for UCD projects shall be fully compatible with the SMS.

The configuration and programming of all panels and devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with UCD Police representatives and shall match the existing naming and classification schema.

B ACCESS CREDENTIALS
Access credentials (cards and fobs) are a foundational part of the ACS. UCD maintains, control over and issues multi-technology cards that function with existing 125MHz proximity card readers as well as newer Smart Card readers. Individual project designed and specified under these Standards should not need to provide access credentials within the scope of work.
C. ACS PANELS

In all circumstances ACS panels shall be fully compatible with and made operational within the existing SMS.

1. ACS Panels should have the following minimum characteristics:
   - ACS panels should be Ethernet capable, utilize an imbedded operating system to provide distributed ACS functionality.
   - ACS panels should be provided with proximity card reader interface capabilities, and input/output functionality.
   - ACS panels should be specified with appropriate panel power supplies, lock power supplies and isolation lock isolation relays. All power supplies should be provided with internal minimum 7amp-hour batteries.

2. Enclosure Tamper Switches
   - If not already equipped from the factory, all ACS panel, power supply and ancillary board enclosures should be equipped with an enclosure tamper switch.
   - Tamper switches should be single-pole, single throw (SPST) units to provide supervision of enclosure doors.
   - Tamper switches shall be tested and proven capable of initiating an alarm signal when the protected door is opened 3/8” on the latch side.
   - Tamper switch should be installed inside the enclosure.

D. ACS and BIAS FIELD DEVICE HARDWARE REQUIREMENTS

1. Card Reader
   - The reader is available in a variety of form factors. The particular form factor that is most suitable to the installation environment should be specified on a per project basis.
   - The reader should be capable of reading and processing the contactless Smart Card and Wiegand Proximity technologies as utilized by UCD.
   - The reader should be read when presented in any orientation or at any angle to the surface of the reader (minimum read range: 3.5”).
   - The reader should power the card, process the encoded data, and output the data to the access system in less than 175 milliseconds.
   - The readers should have an audible “beep” tone feature to indicate to the user that the card or tag was read.
• Accidental or intentional transmission of radio frequency signals into the reader should not compromise the system.
• Damage or vandalism to the reader should not damage any other part of the access control system.
• Individual card reader finishes and colors should be coordinated with the Project Architect and UCD.

2. Door Position Switches/Alarm Contact
• Switches should be single-pole, double throw (SPDT) unit to provide single circuit operation suitable for a line supervision.
• Switches should be capable of initiating an alarm signal when the protected door is opened 1” on the latch side.
• Recessed switches and magnets should be a minimum of 3/8” diameter and a maximum of 1” diameter.
• Surface mount switches should be mounted to door headers and the associated magnet shall be surface mounted to the door.
• Surface mount contacts and magnets should have aluminum housings and be equipped with an armored cable jacket.
• Overhead door contacts should be floor mounted and the associated magnet should be surface mounted to the overhead door.
• Overhead door contacts and magnets should have aluminum housings and be equipped with an armored cable jacket.

3. Request-to-Exit (REX) Devices
• Where feasible, REX devices should be supplied integral with electronic door hardware as defined in the door hardware standards as specified in and coordinated with Division 8.
• REX switches should be single-pole, single throw (SPST) dry micro switch
• In circumstances where it is not feasible for the REX to be integral with the door hardware, a passive infrared motion sensor should be specified.
• Passive infrared REX devices should have an adjustable detection curtain, set to reliably activate prior to an individual exiting but to minimize incidental activation from passersby.
• Individual passive infrared finishes and colors should be coordinated with the Project Architect and UCD.
In circumstances where neither an integral REX nor passive infrared REX is suitable for installation, a push button REX should be utilized.

- REX push button should be mounted to a double gang steel face plate engraved with the words “Push to Release” and the plate shall be installed onto an existing stainless steel pedestal at the applicable door location.
- REX push button should include a DPST dry relay switch.
- REX push button should include a pneumatically controlled adjustable (2-60 seconds) time delay reset.

4. Hardwired Electric Locks
   - Hardwired electric locks should be electrified mortise, cylindrical, strike, rim device, exit device and/or electromagnetic lock as defined by the door hardware standard.
   - Locks should operate at 24 VDC.
   - Locks should have integral REX switch wherever practical.
   - Locks should be provided with appropriate wire transfer or electrified door hinge.
   - Locks should be fail-secure.

5. Wireless Electric Locks
   - For medium security applications wireless electric locks should be utilized.
   - Trim and finish of electric locks should match UCD hardware standards per the project specific requirements and specifications.
   - Wireless locks should incorporate proximity card reader, door position switch and REX device.

6. Emergency Door Release (EDR):
   - EDR should be used in conjunctions with electromagnetic locks where required by local fire code.
   - EDR should be mounted to a single gang stainless steel face plate engraved with the words" Emergency Release".
   - EDR should include a 1-9/16" Red mushroom activation button.
   - EDR should include a pneumatically controlled adjustable (2-60 seconds) time delay reset.
• EDR should include a DPST dry relay switch with one pole hardwired to locally interrupt lock power and the other pole hardwired to the ACS panel and configured as a hardwired input.

7. Motion Detectors
• Motion detectors should be used to provide internal area alarm detection on a time scheduled basis.
• Motion detector should utilize microwave and passive infrared technology to reduce false alarms.
• Motion detector should be surface or flush mount in a standard double gang junction box.

8. Glass Break Detector
• Glass break detectors should be used to provide internal area alarm detection of intrusion attempts though exterior/perimeter glass.
• Glass break detectors should provide low and high frequency detection to reduce the likelihood of false alarms.
• Glass break detectors should be zoned within rooms when complete glass protection requires multiple devices.

9. Microwave Beam Detectors
• Microwave beam detectors should be used to provide internal area alarm detections of intrusion attempts through shy lights, glass roof panels, and/or high ceiling windows that are accessible from the exterior.
• Microwave beam detectors are typically long range devices that include an active unit at one end and a passive unit at the other.
• Where microwave beam detectors are required, infrastructure and architectural coordination will be required.

10. Local Alarm Horn:
• Some perimeter exit doors may be designated as “Emergency Exit Only” and will be equipped with door positions switches/alarm contacts.
• Upon a violation of an emergency exit door, a local horn should be provided to activate a high level sounder. The horn should continue to sound until expiration of the pre-determined software dwell time.
• Horn should deliver a minimum +/-90 peak db.
• Horn must have a sound that is distinguishable from the fire alarm system.

**Video Surveillance System Requirements**

**A. VSS SERVER**
The VSS server is existing. It resides on the UCD Ethernet infrastructure on a dedicated security VLAN. All VSS devices specified in and provided for UCD projects shall be fully compatible with the VSS.

Supplemental server hardware may be required to support the cameras installed as part of the VSS on a given project. When that is the case, the hardware should be provided to exceed the minimum specified requirements for such hardware as published by the manufacturer at the time of design and specification.

The VSS requires each camera in the system to be licensed. Add-on camera licenses should be specified within each project design to accommodate the cameras specified within that particular project.

The configuration and programming of all devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with UCD representatives and shall match the existing naming and classification schema.

**C. VSS DATA STORAGE**
Video data consumes a considerable amount of digital storage. It also requires a considerable amount of network bandwidth, in relation to other network system, to stream video. Therefore, VSS data storage needs to be provided on a per project basis in the form of Network Video Recorders (NVR). The specified storage should be capable of storing all video data, from all project related cameras for a minimum of 30 days, at the following (per-camera) parameters:

- Maximum specified camera resolution
- Minimum four (4) image per second continuous recording
- Minimum fifteen (15) images per second event recording, for the event duration and 10 seconds pre and post event.
D CAMERAS

In all circumstances VSS cameras shall be fully compatible with and made operational within the existing VSS. Specified cameras should meet or exceed the following:

- Cameras should utilize TCP/IP Ethernet with a codec compatible with the existing VSS.
- Cameras should be powered with Ethernet PoE.
- Cameras should use a high resolution, progressive scan, 1/3-inch or greater CMOS imager that provide minimum HD720 (1280x720) pixel resolution.
- Camera resolution should be use based with a minimum HD720 resolution.
- Cameras should be provided with auto-iris, vari-focal lenses with a range applicable to capture the desired field of view.
- Interior cameras should be suitable for interior installation environments.
- Exterior cameras should be suitable for exterior installation environments and should be provided with integral heaters/blowers/seals/etc. necessary to operate in the applicable exterior environment.
- Camera should be as discreet as possible and color, finish and form factor should be closely coordinated with the project architect to balance use and function while maintaining the desired aesthetic of the facility.
This section details the standard protocol to be followed when designing and deploying the SMS sub-system and devices identified in this document. The protocol should be applied to new building, site improvements, and renovations. Deployment considerations include three levels of protection, designated low, medium and high. Such designation can be applied to a room, internal area, or building.

**High Security Designation**

**A**  DEFINITION

High security areas are those that require electronic security devices to provide system monitoring capabilities on a real-time basis. Devices installed in high security areas should be hardwired to ACS and/or BIAS panels or VSS network switch (as appropriate to the specific device) and should be configured and programmed to provide instantaneous alarm/video notification either 24/7 or on a schedule as defined by and coordinated with UCD. Examples of such areas include:

- Ground level access to the first floor building perimeter.
- Computer rooms/data centers
- MDF/MPOE
- High value laboratories
- Administrative areas where cash is transacted
- Senior Administrative Offices
- Physical and electronic records storage areas
- Other locations as defined and designated by UCD

**B**  ACS DEPLOYMENT

The deployment of ACS devices for high security designated areas includes hardwired access controls for the doors that lead into these areas. Hardwired access control doors should include four devices, at a minimum:

- Proximity card reader
- Door position switch/alarm contact
- Electronic lock
- Request-to-Exit device
Doors can also include other ancillary devices, as defined within the door hardware requirements, which should be integrated with the ACS when applied to high security areas. These may include:

- Automatic openers
- ADA openers
- ADA buttons
- Exit devices
- Remote door release buttons

All electronic door hardware devices should be included within the Division 8 specifications for any given project. The security specification should call for close coordination with Division 8. These devices should be electronic version of the locking hardware and devices as defined within the UCD door hardware standard. Whenever feasible, the request-to-exit device should be included as an integral feature of the electronic door hardware. Request-to-exit devices shall not preclude exiting from the interior or require the use of a key, any special knowledge or effort. All security requirements shall conform to California Building Code 1003.3.1.

C  BIAS DEPLOYMENT

BIAS devices can be hardwired or wireless and should be connected to either the ACS or BIAS panel as appropriate to the project. BIAS devices include:

- Door position switch/alarm contact
- Glass Break Detectors
- Motion Detectors
- Beam detectors
- Sonic detectors
- Hold-up Buttons
- Lockdown Buttons
- Duress/Panic Buttons
- Other devices as directed by the UCD

Door position switch/alarm contact should be used on all doors that lead into high security areas but that do not require access control functionality. Furthermore, regular use of the door should be discouraged to prevent nuisance alarms. Therefore, they should be keyed to a building master or grandmaster, in accordance with UCD keying standard.
Glass Break Detectors should be used within high security areas that may be accessible breaking a window, sidelight, or glass panel. The detector should be selected for the particular glass installed. The use of glass break detectors is preferable since they can be armed and operation 24/7 with little risk of false alarm but should be avoided in laboratory environments or other locations where there is a potential of incidental glass breaking. In these areas, motion detectors set on a time schedule of armed through the ACS or BIAS panel should be used.

Beam detectors or sonic detectors should be used to monitor possible intrusion into high security areas by means other than through doors and windows. Skylights, fiberglass wall panels, and block walls are some examples.

Hold-up/panic buttons should be hardwired to the ACS or BIAS panel and should be included in the following locations:

- Financial transaction counters/registers
- Admissions and Records
- Financial Aid
- Library
- Counseling
- Dean’s/Chancellor’s Offices
- Other locations as designated by the UCD

Lockdown button should be hardwired to the ACS or BIAS panel. Lockdown buttons should be configured to lockdown the room, area, floor or building as designated by UCD. In addition, lockdown buttons must be configured as a high priority alarm within the SMS and should be configured to annunciate until acknowledged by a police dispatcher/operator. Lock down buttons that are not primarily designated as hold-up/panic buttons should be included in the following locations:

- Classrooms
- Office reception desks
- Select administrative offices
- Any other area as designated by the UCD

Duress buttons may be hardwired or wireless. While hardwired duress buttons should be used when feasible, wireless buttons are acceptable when hardwiring is not possible or is impractical. Duress buttons are devices that notify police dispatchers of a duress situation is a location
where money is not transacted or where lockdown is not required as a result of button activation. Duress button should be included in the following locations:

- Individual administrative offices where designated by UCD
- Individual faculty offices where designated by UCD
- Locker rooms
- Dressing rooms
- Any other locations as designated by UCD

D VSS DEPLOYMENT

VSS deployment for high security areas chiefly involves the installation of IP based, high definition cameras at strategic locations inside and outside of buildings. Cameras should be included in project designs wherever live and recorded video can effectively supplement ACS and BIAS devices. Typical locations include:

Main exterior pathways around buildings
- Exterior quads/gathering areas
- Exterior approaches to main building entrances
- Interior lobby/corridor/hallways at main entrances
- Interior office lobbies
- Book Store
- All interior counters/windows where duress and holdup buttons are installed which include, but are not limited to:
  - Financial transaction counters/registers
  - Admissions and Records
  - Financial Aid
  - Library
  - Counseling
  - Dean’s/Chancellor’s Offices
- Other areas as designated by UCD

Medium Security Deployment

A DEFINITION

Areas that require electronic security devices to provide system monitoring capabilities on a less than real-time basis are considered medium security. These areas should be equipped with devices that will provide alarm and event tracking data that are primarily used for
investigative purposes and that do not require immediate alarm annunciation and response. Primarily these
areas will be operational within the ACS and will be secured with wireless electronic locks that include integral proximity access control card readers, door status and request-to-exit switches. Video surveillance may be included for these areas as well, but only as directed by UCD. Examples of areas suitable for medium security deployment include:

- Smart classroom (except doors that lead to the building exterior)
- Classrooms that only have exterior doors
- Administration Office Suites and/or Doors (except doors that lead to the building exterior)
- Office with only have exterior door(s)
- IT/Data Closets
- Electrical Rooms
- Mechanical Rooms
- Other medium security rooms as directed by UCD

**Low Security Deployment**

A DEFINITION

Areas that require no electronic security protection but will require mechanical locks as defined in the door hardware standard. Examples of such areas include:

- Closets
- Conference/meeting rooms that do not have doors leading to the building exterior
- General storage rooms
- Offices
- All other rooms and areas not otherwise directed by UCD as medium or high security areas