Design Guidance:

Building Security Systems

Department of Planning+Design+Construction
April 2009
# Table of Contents

**INTRODUCTION**

**GENERAL DESIGN GUIDELINES**

- Access Control ................................................................. 4
- Security Alarms ................................................................. 4
- Burglar Alarms ................................................................. 4
- Holdup Alarms ................................................................. 5
- Duress Alarms ................................................................. 6
- Closed-Circuit Television ................................................... 6
- Local Systems ................................................................. 6
- Central Systems .............................................................. 7
- Emergency Assistance Stations ............................................ 7

**DESIGN AND PROCUREMENT**

- System Design ................................................................. 8
- Schematic Design Phase .................................................... 8
- Design Development Phase ................................................ 8
- Construction Documents Phase .......................................... 8
- Proprietary Issues ........................................................... 8

**SPECIFIC DESIGN GUIDELINES**

- Access Control ................................................................. 9
- Building Perimeter Door Configuration ................................. 9
- Interior Doors ................................................................. 11
- Door Hardware ............................................................... 11
- Programming ................................................................. 14
- Startup and Commissioning .............................................. 14
- Security Alarms ............................................................... 15
- Burglar Alarms ................................................................. 15
- Control Unit ................................................................. 16
- Motion Detectors ............................................................. 17
- Contacts ..................................................................... 17
- Holdup and Duress Switches .............................................. 17
- Wiring Standards ............................................................. 18
- Programming ................................................................. 19
- Startup and Commissioning .............................................. 19
- Closed-Circuit Television Systems ..................................... 20
- Local Systems ................................................................. 20
- Single-Camera System — Event Recording ................................ 20
- Multi-Camera Systems and Time-Lapse Recording .................. 20
- Central CCTV Systems ..................................................... 21
- Startup and Commissioning .............................................. 22
Introduction and Purpose

The University of Cincinnati is committed to providing a safe environment for students, faculty, staff, visitors, and patients. We will use available resources to provide the safest campus possible, while supporting the University’s mission of education, research, and patient care.

The University of Cincinnati is a 24-hour-a-day campus located in a busy urban center. Providing a safe environment while meeting the University’s operational needs is a challenge.

The University supports the use of crime prevention through environmental design (CPTED). CPTED involves design of physical space in the context of the needs of bona fide users, the normal and expected use of the space, and the predictable behavior of both bona fide users and criminals. This is in contrast to the target hardening approach typically used in business and industrial settings. Target hardening often leads to constraints on use, access, and enjoyment of the space, which is antithetical to the University’s goals. This does not mean that UC does not use many of the traditional target hardening tools, such as access control, alarms, and closed-circuit television (CCTV). Rather, these tools are used selectively as they support the University’s mission.
General Design Guidelines

Access Control

All building perimeter doors are controlled by the University access control system. The GE Picture Perfect system is used for card access.

Main and service entrances to buildings will be provided with card access.

Secondary entrances that must be open for public use during normal business hours will be provided with electric locks.

Emergency exits will be monitored to ensure that no doors are being propped open. Emergency exits will have an exterior key access.

Doors intended for emergency exit use only will be provided with delayed egress locking hardware (delay to be no longer than 30 seconds). Areas will be monitored to ensure that doors are not propped open.

No perimeter or public area doors will be designed that require only manual locking or unlocking.

Security Alarms

The University uses the AES IntelliNet alarm system, which is a radio-based packet data communications network. The individual protected areas shall be provided with an AES 7450XL Transceiver. The user interface shall be provided by a Caddx control panel with an AES radio interface.

Burglar Alarms

Burglar alarms shall be installed to protect valuable materials and data from theft by forced entry. The burglar alarm consists of a control panel, user keypad, motion detectors, and door contacts.
General Design Guidelines

The burglar alarm is not a substitute for access control. A burglar alarm is used wherever there is a concentration of material or data whose loss could seriously impact the operation of a unit. Burglar alarms will not use audiovisual alarm devices such as bells, horns, or strobes. Examples of areas that shall be provided with burglar alarm systems are:

- Cash handling areas
- Student and financial records storage areas
- Fine arts storage areas
- Computer server rooms
- Computer labs
- Research labs working with restricted or classified information
- Storage areas for irreplaceable documents or files

Holdup Alarms

Holdup alarms shall be installed to protect personnel handling cash or pharmaceuticals. These alarms are not intended as a general means to summon police assistance; they are to be used only in the event of an armed robbery.

The holdup alarm consists of a control panel and holdup switches, and should normally be paired with a CCTV system. Holdup alarms shall be completely silent and provide no local annunciation of their activation. Examples of areas that shall be provided with holdup alarms are:

- Cashier’s offices
- Pharmacies
- Ticket sales offices
- Restaurant cashiers
- Retail sales counters and cashiers
- Financial services (banks, credit unions)
- Parking booths
General Design Guidelines

Duress Alarms

Duress alarms are installed to protect personnel who may be placed in danger of physical assault during interactions with other persons. Duress alarms are normally placed in locations where an employee may be alone with a potentially threatening person. In areas where other employees are present, the use of a 911 telephone call is preferred.

Duress alarms use the same hardware as holdup alarms and differ only in the intended application. Example areas that shall be provided with duress alarms are:

- Counseling offices
- Psychological service areas
- Emergency medical treatment areas
- Human resources (HR) areas where disciplinary hearings are conducted
- Reception desks for psychological services
- Reception desks for HR
- Reception desks for the President, Vice Presidents, and the Board
- Parking offices

Closed-Circuit Television

Two basic types of CCTV are used at UC:

- **Local recording-only systems** are used where only short-term documentation of activity is needed.

- **The campus central CCTV system**, a matrix system, is used where video must be evaluated in real time by a 911 dispatcher.
Local Systems

Local systems consist of one or more color CCD cameras connected to a digital recorder located at the area being monitored. Local systems shall be installed in the following areas:

- Cash handling/counting rooms
- Cashier's offices in the following areas:
  - Pharmacies
  - Ticket sales offices
  - Restaurant cashiers
  - Retail sales counters and cashiers
- Financial services (banks, credit unions)

Central Systems

Central systems consist of either fixed color closed-circuit display (CCD) or pan/tilt/zoom color CCD cameras connected to the central monitoring facility by fiber optic line. Fixed cameras are used as alarm-activated devices and are tied to either a holdup alarm or an emergency assistance station (EAS). Pan/tilt/zoom cameras shall be installed on building exterior locations so that all major outdoor public areas can be viewed from a camera location.

Emergency Assistance Stations

EAS units are used to provide a means of summoning police assistance. When the activation button on the station is pressed, a two-way audio link with the 911 communications center is opened, and a CCTV camera overlooking the EAS unit is displayed. The EAS system used is manufactured by Simplex.

EAS units shall be installed in garage stairwells that are not glass-enclosed.
Design Guidance: Building Security Systems
April 2009

Design and Procurement

System Design

Schematic Design Phase

When the Schematic Design documents arrive, the UC Public Safety Technical Services Supervisor will assign a Crime Prevention officer and a technician to review the documents for overall space layout and crime prevention issues.

Design Development Phase

When the Design Development documents arrive, the Technical Services Supervisor will review the documents for specific design issues.

Construction Documents Phase

When the Construction Documents arrive, the Technical Services Supervisor will assign a Public Safety technician and a Crime Prevention officer to the project. The Technical Services Supervisor will be responsible for providing coordination with the actual installing contractor(s) and ensuring that the system is brought on-line properly.

Proprietary Issues

The University access control and security alarm systems are proprietary systems, and therefore only GE business partners and AES certified vendors will provide equipment and programming. Wiring and locking hardware are not proprietary and may be provided by the Contractor. The CCTV systems are not proprietary and may be provided by a Contractor who is a manufacturer's authorized installer.
Specific Design Guidelines

Access Control

This section presents specific guidelines for designing the following elements of access control at UC:

- Building perimeter door configuration
- Interior doors
- Door hardware
- Programming

Building Perimeter Door Configuration

Perimeter doors shall be configured for either card access or electric locking.

Card Access: Main entrances to the building shall be equipped with an electric lock controlled by a card reader. Where banks of multiple doors occur, only one door must be equipped with a card reader; the others may be electrically locked only. Where a handicap operator is in place, that door shall always be equipped with a card reader.

Electric Locking: Entrances that need to be open for normal public access but do not need after-hours access shall be equipped with an electric lock, but without a card reader.

Door Position Monitoring

All building perimeter doors, regardless of their locking configuration, will also be equipped with a magnetic contact allowing monitoring of the door position.

Mechanical Key Access

All doors equipped with electric locks shall also be provided with a cylinder for key bypass (emergency access). Doors equipped with magnetic locks shall be provided with a double-pole, double-throw key bypass switch with LED indicators. All locks shall use (7 pin SPIC) Best cylinders for compatibility with the University standard locking system.
Specific Design Guidelines

Control Panel Locations

Control panels for card access (Micro 5 PXN+; Micro 2000 PXN+, Direcdoor) shall be located a maximum distance of 150 feet from the card reader. They may be located up to 250 feet from a controlled door. The Micro shall be located on the same floor as the door they control and shall be placed in the nearest telecommunications closet. Micros may not be placed within 10 feet of power transformers.

For each Micro, a mounting space 2 feet wide by 3 feet high on a ¾-inch plywood backboard shall be provided. A 120VAC, 20A emergency power shall be hardwired to the Micro and associated equipment. A 10baseT UC local area network (LAN) connection shall be provided for each Micro. The Micro communicates across the University LAN. For each control panel a 12-15v lamp power supply (Altronix SMP7PMC+XX) shall be mounted next to control panel for powering the panel.

Card Reader

Card access doors shall be provided with a system compatible card reader mounted on a single gang box located 42 inches above the finished floor. The box and reader shall be mounted vertically. At exterior doors the card reader must be protected from precipitation. If this is not possible, a weather shield should be provided above the reader. All exterior card readers must have a heater unit.

Junction Box

A Micro J Box shall be provided above every door or set of doors that have card access or are controlled. The box shall be located above the finished ceiling where accessible, or immediately below the ceiling.

Wiring

All installations shall use 18 American Wire Gauge (AWG) shielded wire.
Specific Design Guidelines

Interior Doors

Interior doors may be configured for card access using the same hardware listed above for exterior doors. Card access shall be considered for any area that requires either controlled access by large numbers of persons or an audit trail of persons entering the space.

Card Access

Options for interior access control include the use of electrically locked doors and a card reader, as installed on the perimeter doors.

Door Hardware

In the interest of performance and maintainability, specific types of door hardware are recommended for use with the access system. The University standards for door-locking hardware shall also be consulted.

Fire and Panic Hardware

Doors requiring fire or panic hardware shall be provided with University Approved Electrified series hardware in either mortise or rim-locking versions, configured for Fail Secure operation, and with the RX (Request to Exit) option.

The use of vertical rod-locking versions is prohibited because of long-term maintenance problems. The use of E series (electric outside trim) as opposed to EL series (electric latch retraction) is required for fire-rated doors and strongly encouraged for other doors. The EL series is normally used only on doors equipped with a handicap operator, which require the latch to be retracted.

The door hardware schedule must include the appropriate power supply, located within 50 feet of the door. The supply is to be located in an electrical or telephone closet where available, or may be located in an accessible location above the finished ceiling if necessary. The supply must be fed from an emergency power source.
Specific Design Guidelines

“Emergency Exit Only” Doors

Doors that are intended for emergency exit use only, and where an alarm function is needed, shall be provided with VonDuprin CX99 series hardware. Provision must be made to interface the door control with the building fire alarm system in accordance with the National Fire Protection Act (NFPA) 101. This interface is normally accomplished with a Simplex control ZAM located at the lock power supply.

If no delayed egress or alarm function is needed, the standard exit hardware set for the building may be used, with no exterior hardware on the door.

The door hardware schedule must include the appropriate power supply, VonDuprin PS-873+ need modules located within 50 feet of the door. The supply is to be located in an electrical or telephone closet where available, or may be located in an accessible location above the finished ceiling if necessary. The supply must be fed from an emergency power source.

Interior Mortise Locks

Interior doors requiring standard mortise locks should be provided with VonDuprin, CorbinRusswin, or Best hardware. The appropriate 24VDC power supply shall be provided within 50 feet of the door. The supply is to be located in an electrical or telephone closet where available, or may be located in an accessible location above the finished ceiling if necessary. The supply must be fed from an emergency power source. Electric strikes are discouraged because of poor security and reliability.

Power Transfer

Wiring to electric locks shall be by either power transfer (VonDuprin EPT-218) or electric hinge, as appropriate. The use of a power transfer is preferred because it provides greater ease of service in the event repair is required. Power transfers shall be used on new exterior doors. Electric hinges may be used where retrofitting to an existing frame, or for interior wood doors. Door cords are discouraged.
Specific Design Guidelines

**Magnetic Locks**

Magnetic locks may be used in special circumstances, as approved by the Department of Public Safety, Office of Technical Services Supervisor. Such use will require interfacing the magnetic lock with the building fire alarm for emergency door release (Simplex control ZAM located with lock power supply). When the fire alarm is activated, the ZAM must interrupt power to the magnetic lock. The standard magnetic lock is a VonDuprin DS4010HFSL.

The door hardware schedule must include the appropriate power supply, Locknetics 510-EIR, located within 150 feet of the door. The supply must be fed from an emergency power source. The use of magnetic locks also requires that a means of releasing the lock from the interior be provided. A key bypass switch must be provided for emergency bypass of the lock. The switch shall be a VonDuprin SS-901-ISL-MAIN or equivalent and must accept a University Standard Best Cylinder.

**Request-To-Exit Devices**

A request-to-exit device must be provided for all doors that are equipped with an electric or magnetic lock. This device shall normally be a passive infrared detector. Doors utilizing magnetic locks may use a touch bar, Locknetics 690-36-313. In special circumstances a card reader may be used to control exit through a non-designated egress door; however, an emergency break-glass release must be provided (Locknetics 742).

**Spare Parts**

Spare parts shall be provided for all electrical components of the system, in a quantity of 2 percent of the total devices. A minimum of one spare device and a maximum of 10 spare devices of each type will be supplied.
Specific Design Guidelines

Programming

A GE business partner shall program micros to the current UC guidelines. The Public Safety technician assigned to the project will provide this information before programming.

Before the installation, the Micro Ethernet address must be obtained from UCit through Get It. This action should be initiated by the Project Administrator.

Communications from the micro to the host shall be encrypted by triple DES.

Startup And Commissioning

To verify proper operation, the GE business partner shall test each card reader or controlled door in the presence of the assigned Public Safety technician. Testing shall include placing the door in the controlled mode, using a valid card to release the door, using the request-to-exist device to release the door, and placing the door back in the unlocked mode.

Each alarm function of a portal will be tested, including door forced open, door held open, cabinet tamper, AC loss, and low battery.

The Public Safety technician will field-audit the installations to verify that these design standards, including the appropriate wiring practices, have been followed.

The warranty on each micro installation shall commence upon completion of the field audit and University acceptance of the installation.

Commissioning Sheet Addendum A.
Specific Design Guidelines

Security Alarms

This section presents specific guidelines for the following:

- Burglar alarms
- Control unit
- Motion detector
- Contacts
- Holdup and duress switches
- Wiring standards
- Programming

Burglar Alarms

All perimeter doors to the area must be protected with concealed magnetic contacts. Either contacts or interior motion detectors should protect accessible windows. Windows are accessible if they are less than 20 feet above ground level. Motion detectors shall be placed:

- To protect areas containing high-value equipment
- As an interior trap if the room can be entered through a drop ceiling or through windows, or is of drywall construction

Place the keypad(s) inside the main entry door(s). Avoid having a door used for entry if it does not have a keypad nearby. Keypads shall be mounted between 45 and 50 inches AFF. A single protected area shall be contiguous, and the user shall be able to hear the keypad alert from the most remote entry door.

Only upon approval of technical services supervisor can a single system span two floors. Whenever possible, each detection device shall be on a separate zone. No more than three devices of a common type shall be combined on a single zone (i.e., three door contacts). A zone with multiple devices shall cover common or adjacent areas. The system shall be designed to operate a minimum of 8 hours on battery backup.
Specific Design Guidelines

Control Unit

The control unit shall normally be a Caddx NX with an AES interface. The control unit shall protect a single contiguous area, with a maximum of two LCD keypads.

The control panel has eight zones built in; further zones require a zone expander (for an additional 16 zones). One zone is reserved for cabinet tamper protection. No more than three devices should be placed on a common zone. Only devices of the same type (i.e., motion detectors) should be placed on the same zone.

Each control panel shall be paired with an AES IntelliNet subscriber unit.

The control shall be placed inside the protected area, preferably inside a telecommunications closet. If the control unit must be placed in a general storage room, it should be located above the top of the door frame to prevent blockage by stored materials. Placement above a drop ceiling is not desirable. If the control must be located in a room accessible to the general population, it shall be located at least 10 feet AFF.

All control and power supply cabinets shall be protected with tamper switches wired on a 24-hour zone.

All control and power supply cabinets shall be labeled as property of Technical Services and shall display a contact phone number (556-4925).

All plug-in transformers will be secured with a screw or cable tie and will be labeled as above.

Operating instruction signs, showing emergency and service phone numbers, shall be located by each keypad.
Specific Design Guidelines

Motion Detectors

The standard motion detector used shall be a C&K DT-640STC dual tech. Long-range, narrow-beam detection shall use the Sentrol 6155 PIR with 6-degree lens. Detectors shall be placed so that desired movement will be in a diagonal pattern across the detector. The detector shall face the likely entry door.

Detectors shall not be aimed at windows, radiators, fans, etc.

Detectors shall be mounted 7 feet above finished floor.

When possible, detectors will be mounted on a hollow wall and wiring will be concealed within the wall. Whenever possible, detectors shall be mounted on a single gang box or plaster ring.

Contacts

The standard contacts used shall be as follows:

- Sentrol 1078CTW concealed for steel doors
- Sentrol 1125TW concealed for wood doors
- Sentrol 1285TW surface for wood doors where contact cannot be concealed (1045TW for steel doors and frames)
- Sentrol 2515A for overhead doors, gates, and freezers

Contacts shall be installed opposite the hinge side of the door. Surface contacts shall be installed on the secured side. The manufacturer’s installation guidelines will be followed.

Holdup And Duress Switches

The standard switch shall be the HUB25A Momentary Switch. Switches shall be located to limit the potential for accidental activation. Switches located in different rooms must be on separate zones.
Specific Design Guidelines

No other devices shall be connected to the same zone as a holdup or duress switch.

Holdup or duress zones shall be programmed as 24-hour silent zones.

Wiring Standards

All wiring shall be installed in accordance with the current National Electric Code (NEC) and National Fire Protection Association (NFPA) codes.

Plenum cable shall be used in any air-handling ceiling space, unless the cable is run in conduit. When in doubt, use plenum rated cable.

All exposed cable less than 10 feet above the floor will be run in conduit or Wiremold.

Cable run above a drop ceiling shall be laid in cable tray or J-hooks, or otherwise properly secured to structural members. Cable shall not be laid loose above ceiling tiles or tied to conduit or water pipe.

All cable runs shall be numbered on both ends and documented on the as-built drawings.

Cable markings shall be either preprinted labels or Brady machine cable labels. No handwritten labeling shall be used.

The standard cable used will be:

- CL2-P 218/2 for contacts
- CL2-P 18/4 for motions
- CL2-P 18/4 for keypads

End-of-line resistors will be located in series with the last normally closed device on each loop. The location shall be noted on the as-built drawings.

Loop resistance measurements shall be made on each loop, and the values shall be marked on the as-built drawings and inside the control cabinet.

System current calculations shall be marked on the as-built drawings and inside the control cabinet.
Specific Design Guidelines

The location and number of the branch circuit breaker feeding the system shall be marked inside the control cabinet.

All connections shall be made either:
- Under screw terminals;
- With crimp-on connectors, inside a junction box; or
- Soldered and taped, inside a junction box.

Programming

The control shall be programmed for audible entry and exit delays. The entry delay shall be a minimum of 45 seconds. The user should be able to disarm the system after entering from the most remote door. The exit delay shall be a minimum of 60 seconds. The user should be able to arm the system, pick up personal belongings, and exit through the most remote door.

All perimeter doors shall be programmed as entry/exit zones unless there is no exterior hardware on the door. All interior motion detectors shall be programmed as secondary entry/exit zones.

Window contacts shall be programmed as instant zones. Zones shall be programmed for 500 milliseconds. Controls shall be programmed to provide a 24-hour test signal, zone supervision, low battery, and AC power failure.

Startup And Commissioning

To verify proper operation, the AES certified vendor shall test each alarm system in the presence of the assigned Public Safety technician.

Testing shall include placing the panel in the armed mode, tripping each alarm point, and verifying that each zone reports properly.

Each supervisory function of the panel shall be tested, including cabinet tamper, AC loss, and low battery.

The Public Safety technician shall field-audit the installations to verify that these design standards, including the appropriate wiring practices, are followed.
Specific Design Guidelines

The warranty on each alarm installation shall commence upon completion of the field audit and University acceptance of the installation.

Closed-Circuit Television Systems

This section describes requirements for:

- Local CCTV systems
- Single-camera systems
- Multi-camera systems
- Central CCTV systems

Local Systems

Local CCTV systems may comprise one or more cameras, with a digital recording device to allow documentation of activity at the site. Local systems are not monitored at a remote location. Selection of the correct system depends on the amount of video storage needed. The number and location of the cameras used should be designed to ensure complete coverage of the area to be recorded. The final recorded facial image should be no less than one-fifth the total screen height.

Single-Camera System — Event Recording

Single-camera systems where no more than 20 minutes of recorded video activated by an alarm trigger is needed may use the Silent Witness SWC-40 combination video camera and digital recording device. This application is typically used in conjunction with a holdup alarm, where activation of the holdup alarm button also begins the video recording.

Multi-Camera Systems And Time-Lapse Recording

This section addresses situations where more than one camera or ongoing video recording is needed.

The camera used for normally illuminated indoor areas shall be the Sony SSCDC54A 7-inch high-resolution color camera with an appropriate focal length auto iris lens.
Specific Design Guidelines

The camera used for poorly illuminated indoor areas shall be the Sony SSCMX34 7-inch high-resolution black-and-white camera with an integral 12X optical zoom lens.

Wall-mounted cameras shall be installed inside a Pelco EH3508, EMI CCEVH14, or equivalent environmental housing to prevent tampering.

Ceiling-mounted cameras shall be installed inside a Vedolarm RC200c, Vedolarm OH201TL, or equivalent housing.

Camera power shall be provided by an Altronix ALTV244, ALTV2432, or equivalent Underwriters Laboratories (UL)-listed power supply connected to building 120VAC emergency power.

Digital recording shall be provided by a Sony HSR-2 digital video recorder with the appropriate number of camera inputs. The recorder shall be installed inside an EMI SLB2 or equivalent security lock box. Wherever possible, the recorder should be located in the nearest telecommunications closet, either rack-mounted or shelf-mounted. The recorder shall be connected to building 120VAC emergency power.

Monitoring of the digital recorder should be provided by a Sony SSM14 or Pelco PMC14 color monitor, co-located with the digital recorder.

All video connections shall be provided by RG-8 or RG-58 100 percent shielded cable with crimped connectors.

Central Cctv Systems

The central (campus-wide) CCTV system is designed to provide the University 911 dispatcher with the ability to remotely view all major public outdoor areas of the central campus. It uses color pan/tilt/zoom cameras located on top of buildings connected by fiber optic lines to the 911 communications center in Edwards. Number and placement of the cameras is dependent upon specific building design and the associated outdoor spaces, as well as the coverage provided by existing camera locations.

The camera used shall be a Pelco xxx Spectra-Dome color pan/tilt/zoom unit.
Specific Design Guidelines

Cameras shall be located so that they are accessible for normal service without the use of a ladder. The camera shall be mounted using the manufacturer’s parapet mount such that it may be swung back onto the rooftop for service.

The camera shall be connected by the manufacturer’s recommended coaxial and power cabling to the nearest UCit closet containing a fiber optic patch panel. All cable shall be run in conduit.

Camera power shall be provided by a UL-listed power supply meeting the manufacturer's specifications, connected to building 120VAC emergency power.

Surge suppression meeting National Electric Code (NEC) and manufacturer’s specifications shall be provided for both the power and the video cables at the UCit closet.

A Fiber Options xxx converter shall be provided in the UCit closet to convert the video signal from coaxial cable to fiber optic cable.

A Fiber Options xxx converter shall be provided in the 911 Communications Center to convert the video signal from fiber optic cable to coaxial cable.

The camera signal shall be terminated to a designated input of the Pelco switcher located in the 911 Communications Center.

Startup And Commissioning

To verify proper operation, the Contractor shall test each CCTV system in the presence of the assigned Public Safety technician.

Testing of installations with video recording equipment shall include verification of proper video signal, recording, and playback.

Testing of pan/tilt/zoom cameras shall include all remote control operations.

The Public Safety technician shall field-audit the installations to verify that these design standards, including the appropriate wiring practices, are followed.

The warranty on each camera installation shall commence upon completion of the field audit and University acceptance of the installation.

Commissioning Sheet Addendum C