**Recommendation:**  2.3.3 UL Publications. Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.


**Statement:**  The TC updates the referenced standards to the most recent editions.

**Recommendation:**  Text to read as follows:

**** Insert 731_FR 2 Chapter 4 MOS Here ****

**Statement:**  The TC modifies Chapter 4 to comply with the NFPA MOS.
Chapter 4  Fundamentals

4.1  Application.
4.1.1  The provisions of Chapter 4 shall apply to Chapters 5 through 10.
4.1.2  When an electronic premises security system connects to a fire alarm system or other life safety systems, the requirements of other codes and standards pertaining to those systems shall be followed.
4.1.3  When an electronic premises security system is interconnected to an ancillary system, the ancillary system shall not interfere with the operation of the electronic premises security system.

4.2  General.
4.2.1  The provisions of Chapter 4 shall cover the basic functions of an electronic premises security system.
4.2.2  These systems shall be primarily intended to provide notification of alarm, supervisory, and trouble conditions; to alert the occupants; to summon appropriate aid; and to control premises security functions.
4.2.3  Priority of alarm signals over other signals shall be permitted when evaluated by the stakeholders through a risk analysis.

4.3  Equipment.
4.3.1  Equipment constructed and installed in conformity with this standard shall be listed for the purpose for which it is used, in accordance with applicable standards.
4.3.2*  The electronic premises security system components shall be installed in accordance with the manufacturers’ published installation instructions.
4.3.3  Equipment that utilizes initiating, annunciating, and remote control devices that provide signaling by means of low-power radio frequency shall operate in accordance with 47 CFR 15, “Radio Frequency Devices.”
4.3.4*  Equipment that has the physical appearance of a life safety device or appliance but does not perform its apparent life safety function shall be prohibited.

4.4  Personnel Qualifications.
4.4.1  System Design.
4.4.1.1*  Persons who develop plans and specifications in accordance with this standard shall be experienced in the design, application, installation, and testing of electronic premises security systems. Persons who are experienced in the design, application, installation, and testing of electronic premises security systems shall develop plans and specifications in accordance with this standard as required by the AHJ. Persons who are experienced in the design, application, installation, and testing of electronic premises security systems shall develop plans and specifications in accordance with this standard as required by the AHJ.
4.4.1.2  The system designer shall be identified on the system plans and specifications, design documents.
4.4.1.3  Evidence of qualifications shall be provided when requested by the AHJ.
4.4.1.4  Qualified personnel shall include, but not be limited to, one or more of the following:
   (1) Personnel trained and certified by the equipment manufacturer
   (2) Personnel licensed and certified by state or local authority
(3) Personnel certified by an accreditation program or industry-recognized program acceptable to the AHJ
(4) Personnel having completed a formal technical training program arranged by the security system provider and acceptable to the AHJ

4.4.2* System Installation.
4.4.2.1 Installation personnel shall be supervised by persons who are qualified and experienced in the installation, inspection, and testing of electronic premises security systems.
4.4.2.2 Qualified personnel shall include, but not be limited to, one or more of the following:
(1) Personnel trained and certified by the equipment manufacturer
(2) Personnel licensed or certified by federal, state, or local authority
(3) Personnel certified by an accreditation program or industry-recognized program acceptable to the AHJ
(4)* Trained and qualified personnel employed by an organization listed by a national testing laboratory for the servicing of electronic premises security systems

4.5 Power.
4.5.1 Scope. Introduction. The provisions of this Section 4.5 shall apply to power supplies used for electronic premises security systems.
4.5.2 Code Conformance. All power supplies shall be installed in conformity with the requirements of NFPA 70, National Electrical Code, for such equipment and with the requirements indicated in Section 4.5.

4.5.3 Power Supplies Sources.
4.5.3.1 Power supplies shall be installed in conformity with the requirements of NFPA 70, National Electrical Code.
4.5.3.2 Power supplies shall be reliable and of adequate capacity for the intended service.
4.5.3.3* At least two independent power supplies shall be required, one primary and one secondary, for the following electronic premises security systems: (1) Intrusion detection systems (2) Holdup, duress, and ambush systems
4.2.3.2* When required by 4.2.3.1, systems shall be provided with at least two independent and reliable power supplies, one primary and one secondary (standby), each of which shall be of adequate capacity for the application.
4.5.3.4 When installed, secondary power supplies that are not required by 4.5.3.3 shall conform to the requirements of this standard.

4.5.3.1 The following electronic premises security systems shall be required to be provided with at least two independent and reliable power supplies:
(1) Intrusion detection systems
(2) Holdup, duress, and ambush systems
4.5.3.2* When required by 4.5.3.1, systems shall be provided with at least two independent and reliable power supplies, one primary and one secondary (standby), each of which shall be of adequate capacity for the application.

4.5.4 Primary Supply.
4.5.4.1 Primary (main) power shall be supplied either from a dedicated branch circuit or the unswitched portion of a branch circuit by one of the following means:

(1) Commercial light and power
(2) An engine-driven generator or equivalent in accordance with 4.5.7 4.2.9, where a person specifically trained in its operation is on duty at all times
(3) An engine-driven generator or equivalent arranged for cogeneration with commercial light and power in accordance with 4.5.7 4.2.9, where a person specifically trained in its operation is on duty at all times
(4) An alternative energy source such as solar or wind and batteries with capacity as required by the SVA (security vulnerability assessment)

4.5.4.2 The primary supply shall have a high degree of reliability and adequate capacity for the intended service.

4.5.4.3 Circuit disconnecting means shall have a distinctive marking, be accessible only to authorized personnel, and be identified as “PREMISES SECURITY CIRCUIT.”

4.5.4.4 The location of the circuit disconnecting means shall be permanently identified at the premises security control unit.

4.5.4.5 Primary power (main) supplies to equipment that include Class 2 or Class 3 plug-in transformers utilizing receptacles shall be mechanically secured to prevent inadvertent disconnection.

4.5.4.6 An overcurrent protective device of suitable current-carrying capacity and capable of interrupting the maximum short-circuit current to which it could be subjected shall be provided in each ungrounded conductor.

4.5.4.7 A transient voltage surge protection device or circuit shall be installed at or incorporated into the primary power supply for the following:

(1) Microprocessor-based control units
(2) Microprocessor-based subpanels
(3) Microprocessor-based annunciators
(4) Other microprocessor-based equipment

4.5.4.8 Circuit breakers or engine stops shall not be installed in such a manner as to cut off the power for lighting or for operating elevators.

4.5.5 Secondary Supply.

4.5.5.1 The secondary (standby) power supply shall supply energy to the system in the event of total failure of the primary (main) power supply or when the primary voltage drops to a level insufficient to maintain functionality of the control equipment and system components.

4.5.5.2 When primary power is lost or incapable of providing the minimum voltage required for proper operation, the secondary supply shall automatically supply the power to the system without loss of signals or causing transmission of an alarm.

4.5.5.3 For an integrated system, the secondary supply capacity required by 4.5.3.4 4.2.3.2 shall include the load of all premises security-related equipment, functions, or features that are not automatically disconnected upon transfer of operating power to the secondary supply.

4.5.5.4 The secondary supply shall consist of one of the following:

(1) A storage battery dedicated to the electronic premises security system arranged in accordance with 4.5.6 4.2.8
(2) An individual dedicated branch circuit of an automatic-starting engine-driven generator arranged in accordance with 4.5.7 and storage batteries dedicated to the electronic premises security system with 15 minutes of capacity under maximum alarm load.

(3) An emergency generating system as defined in NFPA 70, National Electrical Code, Article 700.

**4.5.5.5** Under maximum quiescent load (system functioning in a nonalarm condition), the secondary supply shall have sufficient capacity to operate an electronic premises security system for a minimum of 4 hours and, at the end of that period, shall be capable of operating all alarm-sounding devices for 15 minutes.

**4.5.5.6** Operation of secondary power shall not affect the required performance of an electronic premises security system.

**4.5.5.7** The system shall produce the same alarm and trouble signals and indications, excluding the ac power indicator, when operating from the standby power source as are produced when the unit is operating from the primary power source.

**4.5.5.8** The secondary power supply shall automatically provide power to the electronic premises security system within 10 seconds, whenever the primary power supply fails to provide the minimum voltage required for operation.

**4.5.5.9** Required signals shall not be lost, interrupted, or delayed for more than 10 seconds as a result of the primary power failure.

**4.5.5.10** Storage batteries dedicated to the electronic premises security system or an uninterruptible power supply (UPS) arranged in accordance with the provisions of NFPA 111, Standard on Stored Electrical Energy Emergency and Standby Power Systems, shall be permitted to supplement the secondary power supply to ensure required operation during the transfer period.

**4.5.5.11** Where a UPS is employed in 4.5.5.10, a positive means for disconnecting the input and output of the UPS system while maintaining continuity of the power supply to the load shall be provided.

**4.5.6 Storage Batteries.**

**4.5.6.1** Batteries shall be permanently marked with the month and year of manufacture, using the month/year format.

**4.5.6.2** Batteries shall be permanently marked with the month and year of installation, using the month/year format.

**4.5.6.3** Batteries shall be replaced in accordance with the recommendations of the electronic premises security equipment manufacturer.

**4.5.6.4** Sealed lead-acid batteries shall be replaced within 5 years of manufacture.

**4.5.6.5** Storage batteries shall be located so that the premises security equipment, including overcurrent devices, are as follows:

1. Readily accessible as defined by NFPA 70, National Electrical Code
2. Not adversely affected by battery gases
3. In accordance with the requirements of NFPA 70, National Electrical Code, Article 480

**4.5.6.6** Cells shall be insulated against grounds and crosses and be mounted securely in such a manner so as not to be subject to mechanical injury by the following means:

1. Mounted in an enclosure approved for the application.
2. Mounted in accordance with 4.7.2.2.
4.5.6.7 Battery racks shall be protected against corrosion.
4.5.6.8 If not located in or adjacent to the electronic premises security system control unit, the batteries and their charger location shall be permanently identified at the premises security control unit.
4.5.6.9 In-line overcurrent protection shall be between the secondary power supply batteries and the secondary power supply.
4.5.6.10 A means shall be provided to automatically maintain the battery fully charged under all conditions of normal operation.
4.5.6.11 A means shall be provided to recharge batteries within 48 hours after fully charged batteries have been subject to discharge.
4.5.6.12 Upon attaining a fully charged condition, the charge rate shall not result in battery damage.
4.5.6.13 The batteries shall be protected against excessive load current by overcurrent devices.
4.5.6.14 The batteries shall be protected from excessive charging current by overcurrent devices or by automatic current-limiting design of the charging source.
4.5.6.15 Supervision means appropriate for the batteries and charger employed shall be provided to detect a failure of battery charging and initiate a trouble signal in accordance with 5.1.1.1.

4.5.7 Engine-Driven Generator Installation. The installation of engine-driven generators shall conform to the provisions of NFPA 70, National Electrical Code, Article 700, and NFPA 110, Standard for Emergency and Standby Power Systems.

4.6 System Functions.
4.6.1 Electronic premises security system functions shall be permitted to be performed automatically.
4.6.2* The performance of electronic premises security system functions shall not interfere with power for fire alarms, for lighting, or for operation of elevators, building control, or other life safety systems.
4.6.3 The performance of electronic premises security system functions shall not preclude the combination of other services requiring monitoring of operations.
4.6.4 Time delays shall be determined by other sections of this standard.
4.6.5 Electronic premises security system alarms, supervisory signals, and trouble signals shall be distinctively and descriptively annunciated.
4.6.6 Equipment shall be designed so that it is capable of performing its intended functions under the following conditions:
   (1) At 85 percent and at 110 percent of the nameplate primary (main) and secondary (standby) input voltage(s)
   (2) At ambient temperatures of 0°C (32°F) and 49°C (120°F)
   (3) At a relative humidity of 85 percent and an ambient temperature of 30°C (86°F)
4.6.7 Equipment intended for use in damp, wet, or exterior environments shall be listed for the use.

4.7 Installation and Design.
4.7.1 General.
4.7.1.1 Where required, the AHJ shall approve system design and installation.
4.7.1.2* The site shall be inspected for environmental factors that affect the operation of the electronic premises security system.
4.7.1.3 The devices installed shall perform their intended functions in the environmental conditions at the protected premises.

4.7.2 Equipment.
4.7.2.1 Devices, appliances, and control units shall be located and mounted so that accidental operation or failure is not caused by vibration or jarring.
4.7.2.2 Unless otherwise permitted by the manufacturer, control units, power supplies, and batteries shall be mounted in the vertical, upright position.

4.7.2.3* All equipment requiring manual resetting to maintain normal operation shall have an indication to the user that the device has not been restored to normal.

4.7.2.4 Equipment shall be installed in locations where conditions do not exceed the voltage, temperature, and humidity limits specified in 4.6.6 unless listed for the application.

4.7.2.5* Control units and subcontrols shall be accessible to service personnel.

4.7.2.6* To reduce the possibility of damage by induced transients, circuits and equipment shall be protected in accordance with the requirements of NFPA 70, National Electrical Code.

4.7.3 Wiring.
4.7.3.1 The installation of all wiring, cable, and equipment shall be performed in a workmanlike manner in accordance with NFPA 70, National Electrical Code, and specifically with Article 725 or Article 800, where applicable.
4.7.3.2 Optical fiber cables shall be protected against mechanical injury in accordance with NFPA 70, National Electrical Code, Article 770.

4.7.3.3* A conductor shall be spliced or joined with a mechanical splicing device listed for this purpose.

4.7.3.4* Unless specifically allowed by the manufacturer's wiring specifications, low voltage electronic premises security system wiring shall be spaced at least 51 mm (2 in.) from conductors of any light and power circuits, unless one of the circuits is in raceway listed for the purpose.

4.7.3.5* Electronic premises security system wiring and cables shall be of the appropriate gauge, strands, insulation, and electrical properties as specified by the equipment manufacturer.

4.7.3.6 Connections of conductors to terminal parts shall ensure a good connection without damaging the conductors and be made by means of pressure connectors, wire binding screws, or splices to flexible leads.

4.7.3.7 Conductors shall be connected to devices and to fittings so that tension is not transmitted to joints or terminals.

4.7.3.8 Wires and cables shall not be placed in such a manner as to prevent access to equipment.

4.7.3.9 Terminals for more than one conductor shall be identified and intended for the purpose.

4.7.3.10 Conductors under a single terminal shall be of the same gauge and composition.

4.7.3.11* Terminals shall be marked or color coded where necessary to indicate the proper connections.
4.7.3.12* All raceway connections to junction boxes and at all open ends of raceway or flexible raceway shall be protected from abrasion and fixed in position in accordance with NFPA 70, National Electrical Code.

4.7.3.13 Circuit identification shall be within the control panel and enclosures used for wiring connections.

4.7.3.14 Circuit identification shall not be visible to the public.

4.7.3.15 Strain relief shall be provided for wiring leaving control panels and junction boxes not utilizing raceway.

4.7.4 Service Loops—Metallic Conductors

4.7.4.1 A minimum 152.4 mm (6 in.) service loop shall be at control panels and enclosures used for wiring terminations.

4.7.4.2 A minimum 152.4 mm (6 in.) service loop shall be at field terminations.

4.7.4.3 Where exposed or subject to damage, service loops shall be mechanically secured.

4.7.5 Service Loops—Optical Fiber Cables.

4.7.5.1 A service loop shall be at control panels and enclosures and field terminations.

4.7.5.2 The radius of the service loop shall meet the manufacturer's specifications.

4.7.5.3 If no manufacturer's specifications exist, the radius shall not be less than 10 times the cable diameter.

4.7.5.4 Where exposed or subject to damage, service loops shall be mechanically protected.

4.8* Low-Powered Radio (Wireless) Systems.

4.8.1* Listing Requirements. Compliance with 4.8.4.5.9 shall require the use of low-powered radio equipment specifically listed for the purpose.

4.8.2 Power Supplies. A primary battery (dry cell) shall be permitted to be used as the sole power source of a low-power radio transmitter where all of the following conditions are met:

(1) Each transmitter shall serve only one device and shall be individually identified at the receiver/fire alarm control unit.

(2) The battery shall be capable of operating the low-power radio transmitter for not less than 1 year before the battery depletion threshold is reached.

(3) A battery depletion signal shall be transmitted before the battery has been depleted to a level below that required to support alarm transmission after 7 additional days of nonalarm operation. This signal shall be distinctive from alarm, supervisory, tamper, and trouble signals; shall visibly identify the affected low-power radio transmitter; and, when silenced, shall automatically re-sound at least once every 4 hours.

(4) Catastrophic (open or short) battery failure shall cause a trouble signal identifying the affected low-power radio transmitter at its receiver/fire alarm control unit. When silenced, the trouble signal shall automatically re-sound at least once every 4 hours.

(5) Any mode of failure of a primary battery in a low-power radio transmitter shall not affect any other low-power radio transmitter.

4.8.3 Alarm Signals.
4.8.3.1* When actuated, each low-power radio transmitter shall automatically transmit an alarm signal.

4.8.3.2* Each low-power radio transmitter shall automatically repeat alarm transmission at intervals not exceeding 60 seconds until the initiating device is returned to its nonalarm condition.

4.8.3.3 Fire alarm signals shall have priority over all other signals.

4.8.3.4 The maximum allowable response delay from activation of an initiating device to receipt and display by the receiver/fire alarm control unit shall be 10 seconds.

4.8.3.5 An alarm signal from a low-power radio transmitter shall latch at its receiver/fire alarm control unit until manually reset and shall identify the particular initiating device in alarm.

4.8.4 Monitoring for Integrity.

4.8.4.1* The low-power radio transmitter shall be specifically listed as using a transmission method that is highly resistant to misinterpretation of simultaneous transmissions and to interference (e.g., impulse noise and adjacent channel interference).

4.8.4.2 The occurrence of any single fault that disables transmission between any low-power radio transmitter and the receiver/fire alarm control unit shall cause a latching trouble signal within 200 seconds.

Exception: Until the expiration date for this exception of June 30, 2013 Until the expiration date for this exception of June 30, 2013, the time period for a low-power radio transmitter with only a single, connected alarm-initiating device shall be permitted to be increased to four times the minimum time interval permitted for a 1-second transmission up to the following

(1) Four hours maximum for a transmitter serving a single initiating device
(2) Four hours maximum for a retransmission device (repeater), where disabling of the repeater or its transmission does not prevent the receipt of signals at the receiver/fire alarm control unit from any initiating device transmitter.

4.8.4.3 A single fault on the signaling channel shall not cause an alarm signal.

4.8.4.4 The periodic transmission required to comply with 4.8.4.2 from a low-power radio transmitter shall ensure successful alarm transmission capability.

4.8.4.5 Removal of a low-power radio transmitter from its installed location shall cause immediate transmission of a distinctive supervisory signal that indicates its removal and individually identifies the affected device.

4.8.4.6 Reception of any unwanted (interfering) transmission by a retransmission device (repeater) or by the main receiver/control unit, for a continuous period of 20 seconds or more, shall cause an audible and visible trouble indication at the main receiver/control unit. This indication shall identify the specific trouble condition as an interfering signal.

4.8.5 Output Signals from Receiver/Control. When the receiver/control is used to actuate remote appliances, such as notification appliances and relays, by wireless means, the remote appliances shall meet the following requirements:

(1) Power supplies shall comply with Chapter 10 or the requirements of 4.8.2.
(2) All the monitoring for integrity requirements of Chapter 10, Chapter 23, or 4.8.4 shall apply.
(3) The maximum allowable response delay from activation of an initiating device to activation of required alarm functions shall be 10 seconds.
(4) Each receiver/control shall automatically repeat alarm transmission at intervals not exceeding 60 seconds or until confirmation that the output appliance has received the alarm signal.
(5) The appliances shall continue to operate (latch-in) until manually reset at the receiver/control.

4.8.2 Power Supplies. A primary battery (dry cell) shall be permitted to be used as the sole power source of a low-powered radio transmitter where all of the following conditions are met:
(1) Each transmitter shall be individually identified at the receiver/control unit.
(2) The battery shall be capable of operating the low-powered radio transmitter for not less than 1 year before the battery depletion threshold is met.
(3) A battery depletion signal shall be transmitted before the battery has been depleted to a level below that required to support alarm transmission after 7 additional days on nonalarm operation.
(4) The battery depletion signal shall be distinctive from alarm, supervisory, and trouble signals; shall visibly identify the affected low-powered radio transmitter; and when silenced, shall automatically re-sound at least once every 4 hours.
(5) A battery failure shall cause a trouble signal identifying the affected low-powered radio transmitter at its receiver/control unit.
(6) When silenced, the trouble signal shall automatically re-sound at least once every 24 hours until the fault condition returns to normal.
(7) Any mode of failure of a primary battery in a low-powered radio transmitter shall not affect any other low-powered radio transmitter.

4.8.3 Alarm Signals.
4.8.3.1* When actuated, each low-powered radio transmitter shall automatically transmit a signal indicating the cause of the activation.
4.8.3.2* Each low-powered radio transmitter shall automatically repeat alarm transmission at intervals not exceeding 60 minutes until the initiating device is returned to its nonalarm condition.
4.8.3.3 The maximum allowable response delay from activation of an initiating device to receipt and display by the receiver/control unit shall be 90 seconds.

4.8.4 Monitoring for Integrity.
4.8.4.1* The low-powered radio transmitter shall be specifically listed as using a transmission method that is highly resistant to misinterpretation of simultaneous transmissions and to interference.
4.8.4.2 Portable wireless devices shall not be required to meet the requirements of 4.8.4.1.
4.8.4.3 The occurrence of a single fault that disables transmission between any low-powered radio transmitter and the receiver/control unit shall cause a latching trouble signal within 200 seconds.

Exception: Where Federal Communications Commission (FCC) regulations prevent meeting the 200-second requirement, the time period for a low-powered radio transmitter with only a single, connected alarm-initiating device shall be permitted to be increased to four times the minimum time interval permitted for a 1-second transmission up to the following:
(1) Four hours maximum for a transmitter serving a single initiating device
(2) Four hours maximum for a retransmission device (repeater) where disabling of the repeater or its transmission does not prevent the receipt of signals at the receiver/control unit from any initiating device transmitter.

4.8.4.4 A single fault on the signaling channel shall not cause an alarm signal.

4.8.4.5 The periodic transmission required to comply with 4.8.4.3 4.5.9.4.3 from a low-powered radio transmitter shall ensure successful alarm transmission capability.

4.8.4.6 Removal of a low-powered radio transmitter from its installed location shall cause a signal that indicates its removal and identifies the affected device.

4.8.4.7 The requirement of 4.8.4.6 4.5.9.4.6 shall not apply to dwelling unit electronic premises security systems.

4.8.4.6 Reception of any unwanted (interfering) transmission by a retransmission device (repeater) or by the main receiver/control unit for a continuous period of 20 seconds or more shall cause an audible and visible trouble indication at the main receiver/control unit.

4.8.4.7 The trouble indication shall identify the specific trouble condition as an interfering signal.

4.8.4.8 When the receiver/control is used to actuate remote appliances, such as relays, by wireless means, the remote appliances shall meet the following requirements:

(1) Power supplies shall comply with Chapter 4 or the requirements of 4.8.2 4.5.9.2.

(2) All supervision requirements of Chapter 4 or 4.8.4 4.5.9.4 shall apply.

(3) The maximum allowable response delay from activation of an initiating device to activation of required alarm functions shall be 90 seconds.

(4) Each receiver/control shall automatically repeat alarm transmission at intervals not exceeding 60 seconds or until confirmation that the output appliance has received the alarm signal.

(5) The appliances shall continue to operate (latch in) until reset at the control.

4.9 Grounding.

4.9.1 All grounding shall be in accordance with NFPA 70, National Electrical Code.

4.9.2 Additional grounding shall be in accordance with manufacturer's requirements.

4.9.3 All other circuits shall test free of grounds.

4.10 Zoning and Annunciation.

4.10.1* All required annunciation means shall be readily accessible to responding personnel and shall be located as required by the AHJ to facilitate an efficient response to the event.

4.10.2* When required, the location of an operated initiating device shall be visibly indicated by building, floor, or other approved subdivision by annunciation, printout, or other approved means.

4.10.3 When required, the visible indication shall not be canceled by the operation of an audible alarm silencing means.

4.10.4* Visual annunciators shall be capable of displaying all locations in alarm.

4.10.5 If all locations in alarm are not displayed simultaneously, visual indication shall show that other locations are in alarm.

4.11 Testing. All electronic premises security systems shall be maintained and tested in accordance with Chapter 10.

4.12 Software Control.
4.12.1 Where required, all software provided with an electronic premises security system shall be listed for use with the equipment on which it is installed.

4.12.2* A record of installed software version numbers shall be maintained at a location acceptable to the AHJ.

4.12.3* All software shall be protected from unauthorized changes.

4.12.4 All changes shall be tested in accordance with Chapter 10.

4.13 System Requirements.

4.13.1 General.

4.13.1.1 Electronic premises security systems shall be permitted to be either integrated systems combining all detection, notification, and auxiliary functions in a single system or a combination of component subsystems.

4.13.1.2 Electronic premises security system components shall be permitted to share control equipment or to be able to operate as stand-alone subsystems that are arranged to function as a single system.

4.13.1.3 All component subsystems shall be capable of simultaneous, full-load operation without degradation of the required, overall system performance.

4.13.1.4 Where required by other sections of this standard, additional power supplies provided for control units, circuit interfaces, or other equipment essential to system operation, located remote from the main control unit, shall comprise a primary power supply and a secondary power supply that shall meet the requirements of 4.5.34.2.3 through 4.5.64.2.8.

4.13.1.5 Where required, the method of interconnection of control units shall meet the monitoring requirements of Chapter 5; comply with NFPA 70, National Electrical Code; and be achieved by one of the following recognized means:
   (1) Electrical contacts listed for the connected load
   (2) Listed digital data interfaces such as serial communications ports and gateways
   (3) Other listed methods

4.13.1.6 If approved by the AHJ, interconnected control units providing localized detection, signaling, and ancillary functions shall be permitted to be monitored by an electronic premises security system as initiating devices.

4.13.1.7 Each interconnected control unit shall be separately monitored for alarm, trouble, and supervisory conditions.

4.13.1.8 Interconnected control unit alarm signals shall be permitted to be monitored by zone or combined common signals.

4.13.2 Combination Systems.

4.13.2.1 Systems other than electronic premises security systems shall be permitted to share components, equipment, circuitry, and installation wiring with premises security systems.

4.13.2.2 To maintain the integrity of electronic premises security system functions, the provision for removal, replacement, failure, or maintenance procedure on any supplementary hardware, software, or circuit(s) shall not impair the required operation of the electronic premises security system.

4.13.2.3 If the AHJ determines that the information being displayed or annunciated on a combination system is excessive and is causing confusion and delayed response to an emergency, the AHJ shall be permitted to require a separate display or annunciation of information for the electronic premises security system.
4.14 Documentation and Training.
4.14.1.1 The AHJ shall be notified prior to the start of installation, if required.
4.14.1.2 Notification of alteration of equipment or wiring shall be provided to the AHJ, if requested.
4.14.1.3 At the AHJ's request, complete information regarding the system or system alterations, including specifications and battery calculations, shall be provided.
4.14.1.4 Before requesting final approval of the installation, if required by the AHJ, the installing contractor shall verify that the system has been installed in accordance with the system design and tested in accordance with the manufacturer's published instructions.

4.14.2* Documentation. Every system shall include the following documentation, which shall be delivered to the party responsible for the protected premises upon final acceptance of the system:

(1)* Owner's manual
(2) User's instructions
(3)* A record of completion by the system installer
(4) Name and contact telephone number of the organization maintaining the electronic premises security system
(5) Name and contact telephone number of the organization monitoring the electronic premises security system displayed at the control unit
(6) Any other documentation required by law or the AHJ

4.14.3 Training.
4.14.3.1* The party responsible for the protected premises shall arrange for an appropriate level of training of the system users.
4.14.3.2* The user training shall be documented and maintained for 1 year, with the system documentation made available to the AHJ upon request.
6.1.5 Locking Systems.

6.1.5.1* Control of egress shall comply with the requirements of the applicable codes and standards based on the occupancy and usage of the facility.

6.1.5.2* Locking systems shall be installed in accordance with the manufacturer's instructions.

6.1.5.3 Installation of locking hardware on swinging, sliding, and overhead fire-rated door assemblies shall be in accordance with the listing of the doors and frames, in compliance with NFPA 80, Standard for Fire Doors and Other Opening Protectives.

6.1.5.4* Portals shall automatically secure where the portal is supervised by the access control system.

6.1.5.5* Where a delayed egress function is used in conjunction with an access control system, equipment shall be listed for the purpose and be installed in accordance with the applicable codes and standards based on the occupancy and usage of the facility.

6.1.5.6 Where a portal is a required means of egress and is provided with an active lock, the locking system shall comply with 6.1.5.6(1) OR (2) except as otherwise permitted by 6.1.5.7:

(1) Manual Request to Exit (RTE) on Door. A manual RTE device meeting all of the following criteria shall be provided:
   (a) The manual RTE device shall be provided on the egress side of the portal.
   (b) The manual RTE device shall be positioned on the door leaf, gate, or other physical barrier at the portal egress opening.
   (c) The manual RTE device, when operated, shall result in direct release of the active lock, independently of the access control system, in the direction of egress.

(2) Automatic RTE and a Manual RTE Not on Door. An automatic and a manual RTE device meeting all of the following criteria shall be provided:
   (a) The automatic RTE device shall be provided on the egress side, arranged to detect an occupant approaching the portal, to release the active lock in the direction of egress upon detection of an approaching occupant.
   (b) The manual RTE device shall be provided to meet all of the following criteria:
      i. The manual RTE device shall be provided on the egress side of the portal.
      ii. The manual RTE device shall be located 1015 mm to 1220 mm (40 in. to 48 in.) vertically above the floor and within 1525 mm (60 in.) of the portal.
      iii. The manual RTE device shall be readily accessible and clearly identified by a sign that reads: “PUSH TO EXIT.”
      iv. The manual RTE device, when operated, shall result in direct release of the active lock, independently of the access control system, in the direction of egress.

6.1.5.7* The means of lock release required for egress portals by 6.1.5.6 shall not be required as follows:

(1) Where allowed by applicable codes

(2) Where approved by the AHJ

Statement: The TC edits the text for compliance with the NFPA Manual of Style.
731- Log #FR8  
(7.2.3) 

**Final Action:**

**Submitter:** Technical Committee Premises Security  
**Recommendation:** Text to read as follows: 

7.2.3  The level of vandal resistance shall be determined by the SVA risk assessment or the requirements of the AHJ.

7.2.4 In the absence of an SVA risk assessment or AHJ requirement, consideration shall be given to protecting the cameras from being impaired by vandalism.

**Statement:** The TC changes risk assessment to SVA for consistency.

---

731- Log #FR5  
(10.5.3) 

**Final Action:**

**Submitter:** Technical Committee Premises Security  
**Recommendation:** Text to read as follows: 

10.5.3  As an alternative means of compliance with 10.5.1 or 10.5.2, subject to the approval of the AHJ, electronic premises security systems shall be permitted to be inspected, tested, and maintained under a written performance-based program.

10.5.3.1 Goals established under a performance-based program shall provide assurance that the electronic premises security systems will perform its intended functions.

10.5.3.2 Technical justification for the inspection, testing, and maintenance intervals shall be documented.

10.5.3.3 The performance-based option shall include historical data acceptable to the AHJ.

10.5.3.4 Documentation of performance-based testing shall be in accordance with 10.6.

**Statement:** The TC accepts the submitter's concept as presented in Log #1 and revises for completeness. Performance-based testing is not meant to reduce testing requirements but to allow other methods to ensure the same reliability of the installed system.

The TC does not necessarily agree with the submitter's substantiation because performance-based testing applies to other than educational occupancies.

---

731- Log #FR13  
(A.4) 

**Final Action:**

**Submitter:** Technical Committee Premises Security  
**Recommendation:** Text to read as follows: 

**** Insert 731_FR 13 Chapter 4 Annex MOS Here ****

**Statement:** The TC revises the Annex references for consistency and to correlate with FR# 2.
The intent of this paragraph is that those devices that receive power from a two-wire circuit, initiating device circuit, or addressable device circuit must be listed for use with that control panel. It is not the intent of this paragraph to require a compatibility listing for those devices that receive power only from the auxiliary power outputs of the control panel or remote power supply. The system designer does need to be aware of the voltage and current requirements and limitations of both the control unit and the devices powered from the auxiliary output.

The presence of an apparent life safety device or appliance creates an expectation that these safety features are functional, resulting in a false sense of security. It is not the intent to prohibit listed devices that can perform both functions.

Examples of qualified personnel include individuals who can demonstrate experience on similar systems that they have designed.

The installers of electronic premises security systems should be familiar with the equipment that they are to install. This includes knowing the application limits of the devices and appliances for a particular design. The installer should have an understanding of the causes of false alarms and methods that can be taken to decrease the possibility of their occurrence.

There are various levels of recognized accrediting organizations. They range from those that accredit the installation company to those that issue certifications for the installers. They are not necessarily equal. Each program should be examined to verify that it meets the intent of the interested parties and applicable laws governing the type of system being installed.

There are various levels of recognized accrediting organizations. They range from those that accredit the installation company to those that issue certifications for the installers. They are not necessarily equal. Each program should be examined to verify that it meets the intent of the interested parties and applicable laws governing the type of system being installed.

The designer for other electronic premises security systems can include secondary power requirements, depending on the risk assessment and design objectives of the systems.

Secondary power for electronic premises security systems can be based on the SVA risk assessment and the design. Consideration should be given to whether access to the system is readily available and to the property being protected. For example, if a standby power source were to be installed in a vault with a time lock mechanism, the capacity of the standby power should exceed the time lock. The designer should be aware of other standards that can require additional battery capacity.

When an electronic premises security system is used in conjunction with egress control, consideration should be given to building and fire codes.
Examples of environmental factors that should be considered include, but are not limited to, the following:

1. Fog
2. Rain
3. Snow
4. Humidity and corrosion
5. Cold and heat
6. Vibration
7. Radio frequency interference (RFI)
8. Electrical discharge
9. Ac induction
10. Dust
11. Smoke
12. Animals and insects
13. Vegetation
14. Decorations and marketing aids

The means of indication might be the failure to arm the system until the manually reset device is restored to its normal condition.

Additional information on this subject can be found in NFPA 70, National Electrical Code, Article 110.

The system designer and the installer should be aware that induced transients such as line noise or ac voltage could be injected into an electronic premises security system. NFPA 70, National Electrical Code, provides methods for preventing these induced transients from being injected into the system. The system designer and the installer should be familiar with all of NFPA 70, National Electrical Code, and in particular, Chapters 3, 6, and 8, regarding this topic.

A splice intended to be soldered should be joined mechanically before being soldered. Each splice and joint should be covered either with insulation equivalent to that of the conductors or with not less than two layers of electrical tape. A splice located in an area of dampness should be treated with a listed sealant or be equivalently treated.

Electrical connections to a device manufacturer's supplied leads should be either of the following methods:

1. Soldered and heat shrink–wrapped
2. Crimped with a listed insulating crimp connector

Care should be taken to ensure that each connection between a device's leads and a wire or cable provides the required strain relief.

Electrical connections to terminals on a device should be made by first crimping or soldering spade, tinned wire, or “O”-type connection terminals of a size appropriate to the device's terminals to the conductors from the wires or cables. These connection terminals should be insulated either by manner of their construction and use or by adding heat shrink over the connection for each individual connector. Poorly performed connections that do not include all the strands of the conductor, that are bent or misshapen, or that do not properly fit the terminals on the device are not acceptable. Care should be taken to ensure that each connection between a device and the wire's
or cable’s conductors provides adequate strain relief so that a firm tug does not break or damage the connection.

A.4.5.8.3 A.4.7.3.4 The intent of this requirement is to shield the wiring from induction of ac, in accordance with NFPA 70, National Electrical Code.

A.4.5.8.4 A.4.7.3.5 Consideration should be given to selecting appropriate cables in areas that require flexibility of the conductors, such as pole-to-pole cables and elevator traveling cables. Cables might need to have a special listing for applications such as aerial cable.

A.4.5.8.5.6 A.4.7.3.11 The intent of this requirement is to assist service technicians who might not have been the installer installed the system so that they can quickly identify circuits that might be in trouble. Terminal identification can be a schematic on the inside of the control panel door.

A.4.5.8.6 A.4.7.3.12 Some examples of properly mounted devices and protected cables are as follows:

(1) If a field device is not mounted on a back box to which raceway can be attached, and it is not possible to provide such a box, then wiring should be protected from abrasion at the raceway end or enclosure. The device and the metal raceway should not be more than 76.2 mm (3 in.) apart.

(2) The orientation of the installed metal raceway relative to the installed device should be so as to facilitate removal, reconnection of a replacement, and reinstallation without the need to damage any finished surfaces or extend time fishing for wires or cables. Generally, such metal raceway should be installed so that its extension would be roughly perpendicular to the finished surface in which the device is installed.

(3) Wire or cable ends at the point of connection to a device should have the outside protective sheathing removed so that the ends of the internal insulated conductors extend at least 50.8 mm (2 in.). The wires or cables should be cut so that, including the stripped end, they extend at least 152.4 mm (6 in.) beyond the finished surface at the point of device installation. Where inserting the cut cable back into the opening is difficult, additional stripping of outside sheathing is acceptable. Removal of the outside sheathing should be performed without damaging the insulation of the internal conductors of the wires or cables. In some cases, manufacturers can provide unique instructions for their product. Stripping of sheathing is not necessarily an acceptable practice with products such as coaxial cable or category network cable.

(4) Conductors should be stripped to the length prescribed by the manufacturer of the device to which the conductors should be connected. The stripped portion of the conductor should have the same number of conductors as the unstripped portion.

A.4.5.9 A.4.8 The term low-powered is used to eliminate potential confusion with other transmission media, such as optical fiber cables.

Low-powered radio devices are required to comply with the applicable low-power requirements of 47 CFR 15, “Radio Frequency Devices.”

A.4.5.9.1 A.4.8.1 Equipment listed solely for dwelling units use would not comply with this requirement.

A.4.5.9.3.1 A.4.8.3.1 This requirement is not intended to preclude verification and local test intervals prior to alarm transmission.
The Federal Communications Commission (FCC) treats alarm retransmission in a very specific way. The following is an extract of the FCC requirements in 47 CFR 15, Section 15.231:

“Periodic operation in the band 40.66 – 40.70 MHz and above 70 MHz

(1) The provisions of this section are restricted to periodic operation within the band 40.66—40.70 MHz and above 70 MHz. Except as shown in paragraph (e) of this section, the intentional radiator is restricted to the transmission of a control signal such as those used with alarm systems, door openers, remote switches, etc. Continuous transmissions, voice, video and the radio control of toys are not permitted. Data is permitted to be sent with a control signal. The following conditions shall be met to comply with the provisions for this periodic operation:

(a) A manually operated transmitter shall employ a switch that will automatically deactivate the transmitter within not more than 5 seconds of being released.
(b) A transmitter activated automatically shall cease transmission within 5 seconds after activation.
(c) Periodic transmissions at regular predetermined intervals are not permitted. However, polling or supervision transmissions, including data, to determine system integrity of transmitters used in security of safety applications are allowed if the total duration of transmissions does not exceed more than 2 seconds per hour for each transmitter. There is no limit on the number of individual transmissions, provided the total transmission time does not exceed 2 seconds per hour.
(d) Intentional radiators which are employed for radio control purposes during emergencies involving fire, security, and safety of life, when activated to signal an alarm, may operate during the pendency of the alarm condition.
(e) Transmission of setup information for security systems may exceed the transmission duration limits in paragraphs (a)(1) and (a)(2) of this section, provided such transmission are under the control of a professional installer and do not exceed 10 seconds after a manually operated switch is released or a transmitter is activated automatically. Such setup information may include data. In addition, devices operated under the provisions of this paragraph shall be provided with a means for automatically limiting operation so that the duration of each transmission shall not be greater than 1 second and the silent period between transmissions shall be at least 30 times the duration of the transmission but in no case less than 10 seconds.”

Examples of interference are impulse noise and adjacent channel interference.

The primary purpose of electronic premises security system annunciation should be to enable responding personnel to identify the location of an event quickly and accurately.

Ideally, one zone should be dedicated to each detection device. If more than one device resides on a zone, the area covered by all zone devices should not exceed the area that one person can maintain under surveillance from a single location.

If the system serves more than one building, each building should be indicated separately.
The installed software version number can be located at or within the electronic premises security system or it can be kept elsewhere within the protected premises. The AHJ is to be made aware of the location, and if it is acceptable an alternate location can be used.

A commonly used method of protecting against unauthorized changes can be described as follows (in ascending levels of access):

1. **Access Level 1**, which is access by persons who have a general responsibility for safety supervision and who could be expected to investigate and initially respond to an electronic premises security alarm or trouble signal
2. **Access Level 2**, which is access by persons who have a specific responsibility for safety and security and who are trained to operate the electronic premises security system
3. **Access Level 3**, which is access by persons who are trained and authorized to do the following:
   - Reconfigure the site-specific data held within or controlled by the electronic premises security system
   - Maintain the electronic premises security system in accordance with the manufacturer's published instructions and data
4. **Access Level 4**, which is access by persons who are trained and authorized either to repair the electronic premises security system or to alter its site-specific data or operating system program, thereby changing the basic mode of operation

Examples of parties responsible for the protected premises include, but are not limited to, the owner of the protected property, the leaseholder of the tenant space where the system is installed, and an employee or agent of the owner or the leaseholder.

Documentation that can compromise the electronic premises security system should be protected in such a way as to prevent the unauthorized release of critical system locations, operations, and functions.

The owner's manual should include the following:

1. A detailed narrative description of the system inputs, signaling, ancillary functions, annunciation, intended sequence of operation, expansion capability, application considerations, and limitations
2. Operator instructions for basic system operations, including alarm acknowledgement, system reset, interpretation of system outputs (LEDs, CRT display, and printout), operation of manual ancillary function controls, and change of printer paper
3. A detailed description of routine maintenance and testing as required and recommended, as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed, and that includes the following:
   - Listing of the individual system components that require periodic testing and maintenance
   - For each type of device installed, step-by-step instructions detailing the requisite testing and maintenance procedures and the intervals at which these procedures should be performed
(c) A schedule that correlates the testing and maintenance procedures recommended in Chapter 10
(d) Troubleshooting instructions that detail each trouble condition generated from monitored field wiring, including opens, grounds, and loop failures, and that include a list of all trouble signals annunciated by the system, a description of the condition(s) that cause such trouble signals, and step-by-step directions describing how to isolate such problems and correct them or call for service, as appropriate
(e) A service directory, including a list of company names and emergency (24/7/365) telephone numbers of those companies providing service for the system A.4.7.2.1(3) A.4.14.2(3) Many installers have their own record of completion forms. Examples of record of completion forms are shown in Figure A.4.7.2.1(3)(a) A.4.14.2(3)(a) through Figure A.4.7.2.1(3)(e) A.4.14.2(3)(e).
# RECORD OF COMPLETION INSPECTION & TESTING REPORT

Date: ____________  Time: ____________

### Protected Premises:
Name: __________________________
Address: ________________________
Representative: __________________
Signature: _______________________
Telephone: _______________________

### Alarm Service Company:
License #: ______________________
Name: __________________________
Address: ________________________
Representative: __________________
Signature: _______________________
Telephone: _______________________

### TYPE OF SYSTEM (check all that apply)
- Exterior intrusion detection
- Access control
- Interior intrusion detection
- Holdup, duress, or ambush

(Attach an Inspection & Test Report for each type of system checked above.)

### DESCRIPTION OF TRANSMISSION

#### Off-Premises Monitoring:
- Central station
- Proprietary station
- Law enforcement center
- None

#### Monitoring Station:
Name: __________________________
Address: ________________________
Telephone: _______________________

#### Type of Transmission (indicate the number of each type provided):
- Digital
- Cellular
- Long-range radio
- Data packet network
- Direct wire
- Multiplex
- Derived channel
- Other

#### Transmitters:
Mfr.: ____________________________
Model: __________________________
Transmission type: ________________

#### SYSTEM POWER SUPPLIES

Primary (Main):
- Nominal voltage: _____________  Amps: __________
- Overcurrent protection: Type: ____________  Rating: __________
- Location of disconnecting means: ________________________
- Disconnecting means (panel and breaker number): __________

Secondary (Standby):
- Battery:  None
- Hours of backup battery (calculated capacity): __________
- Number of batteries: ____________
- Date of battery mfg.: ____________
- Last replacement date: __________
- Battery size (AH): ____________
- Type of battery: ____________
- Next replacement date: __________

#### Engine-Driven Generator
- Number of generators: __________
- Automatic starting:  Yes  No
- Location: ______________________
- Party responsible for testing: _____________________
- Test frequency: __________________
- Date of last test: __________________
- Transfer switch location: ___________________
- Manual or Automatic (M/A): __________

© 2010 National Fire Protection Association

FIGURE A.4.7.2.1(3)(a) A.4.14.2(3)(a) Sample Record of Completion Report.
### Intrusion Detection or Holdup and Duress Systems Inspection & Testing Report

#### System Description

**Type of System:**
- Exterior intrusion detection
- Interior intrusion detection
- Holdup system
- Duress system
- Ambush system

**Control Unit:**
- **Mfr.:**
- **Model:**

**Type of Circuit:**
- End of line Number of circuits: __________
- Addressable Number of addresses: __________
- Wireless Number of transmitters: __________

#### Detection Devices

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Type of Detection</th>
<th>Device Type or Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audio sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contacts — door</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contacts — window</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exterior buried detectors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Motion detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Photoelectric detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pressure &amp; stress sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective cable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective wiring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Proximity sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shock sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sound detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Holdup devices — portable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Holdup devices — fixed in place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Duress devices — portable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Duress devices — fixed in place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ambush devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

#### Signaling Devices

<table>
<thead>
<tr>
<th>Location</th>
<th>Quantity</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interior</td>
<td>__________</td>
<td>Bell</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Siren</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Horn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Exterior</td>
<td>__________</td>
<td>Bell</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Siren</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Horn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
</tbody>
</table>

### Notification of Testing

Notify party responsible for the protected premises:
- **Name:**
- **Date:**
- **Time:**

**Monitoring station:**
- **Name:**
- **Date:**
- **Time:**

© 2010 National Fire Protection Association

**FIGURE A.4.7.2.1(b) A.4.14.2(3)(b)**  Sample Intrusion Detection or Holdup and Duress Systems Report.
## SYSTEM INSPECTION AND TEST

<table>
<thead>
<tr>
<th>Component</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arming means</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary power circuit disconnect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary power</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Batteries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voltage at end of test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generator records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signaling device(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protective circuit supervision</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## DETECTION DEVICE INSPECTION AND TEST

<table>
<thead>
<tr>
<th>Location/Address</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Results/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Attach additional sheets as necessary to list all devices.)

© 2018 National Fire Protection Association

**FIGURE A.4.7.2.1(b) A.4.14.2(3)(b) Continued**
TRANSMISSION TEST

<table>
<thead>
<tr>
<th>Signal/Component</th>
<th>Yes</th>
<th>No</th>
<th>Time</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm signal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisory signal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trouble signal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FINAL TEST REPORT

The following did not operate properly:


NOTIFICATION OF END OF TESTING

Notify party responsible for the protected premises:

Name: ___________________________ Date: ___________ Time: ___________

Monitoring station:

Name: ___________________________ Date: ___________ Time: ___________

System restored to normal operation: ___________________________

Date: ___________ Time: ___________

Testing was performed in accordance with applicable NFPA standards.

Name of inspector: ___________________________ Date: ___________

Signature: ___________________________ Time: ___________

Party responsible for the protected premises:

Name: ___________________________ Date: ___________

Signature: ___________________________ Time: ___________

© 2010 National Fire Protection Association

FIGURE A.4.7.2.1(b) A.4.14.2(3)(b) Continued
## ACCESS CONTROL
### INSPECTION & TESTING REPORT

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Type of Components</th>
<th>Device Type or Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power supply</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reader</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magnetic stripe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RFID card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Biometric</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Position sensor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electric latch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electric lock</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electromagnetic lock</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Request to exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Motion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

### NOTIFICATION OF TESTING

Notify party responsible for the protected premises:

Name: ___________________________ Date: __________ Time: __________

Monitoring station:

Name: ___________________________ Date: __________ Time: __________

### SYSTEM INSPECTION AND TEST

<table>
<thead>
<tr>
<th>Component</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary power circuit disconnect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary power</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Batteries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voltage at end of test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generator records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power supply</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2010 National Fire Protection Association  
NFPA 731 (p. 1 of 3)

FIGURE A.4.7.2.4(c) A.4.14.2(3)(c) Sample Access Control Report.
## COMPONENT INSPECTION AND TEST

<table>
<thead>
<tr>
<th>Location/Address</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Results/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Attach additional sheets as necessary to list all devices.)

FIGURE A.4.7.2.1(e) A.4.14.2(3)(c) Continued
# ACCESS CONTROL

**INSPECTION & TESTING REPORT** *(continued)*

## TRANSMISSION TEST

<table>
<thead>
<tr>
<th>Signal</th>
<th>Yes</th>
<th>No</th>
<th>Time</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm signal</td>
<td>☑️</td>
<td>☐</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trouble signal</td>
<td>☑️</td>
<td>☐</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## FINAL TEST REPORT

The following did not operate properly:

- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

## NOTIFICATION OF END OF TESTING

Notify party responsible for the protected premises:

Name: __________________________ Date: ___________ Time: ___________

Monitoring station:

Name: __________________________ Date: ___________ Time: ___________

System restored to normal operation: __________________________ Date: ___________ Time: ___________

**Testing was performed in accordance with applicable NFPA standards.**

Name of inspector: __________________________ Date: ___________

Signature: __________________________ Time: ___________

Party responsible for the protected premises:

Name: __________________________ Date: ___________

Signature: __________________________ Time: ___________
# VIDEO SURVEILLANCE
## INSPECTION & TESTING REPORT

### COMPONENTS

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Type of Components</th>
<th>Device Type or Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Video controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video switcher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video multiplexer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitor (monochrome or color)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recorder (Tape or DVR)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enclosure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pan tilt zoom (PTZ)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alarming inputs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

### NOTIFICATION OF TESTING

Notify party responsible for the protected premises:

- Name: ____________________________  Date: ___________  Time: ___________
- Monitoring station:
  - Name: ____________________________  Date: ___________  Time: ___________

### SYSTEM INSPECTION AND TEST

<table>
<thead>
<tr>
<th>Component</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control unit</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Primary power circuit disconnect</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Secondary power</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Batteries</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Voltage at end of test</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Generator test records</td>
<td>☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Remote controls</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
<tr>
<td>Variable lenses</td>
<td>☐ ☐ ☐ ☐</td>
<td>☐ ☐ ☐ ☐</td>
<td></td>
</tr>
</tbody>
</table>

© 2010 National Fire Protection Association

NFPA 731 (p. 1 of 2)

**VIDEO SURVEILLANCE**
**INSPECTION & TESTING REPORT (continued)**

**COMPONENT INSPECTION AND TEST**

<table>
<thead>
<tr>
<th>Location/Address</th>
<th>Visual Check</th>
<th>Functional Test</th>
<th>Results/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Attach additional sheets as necessary to list all devices.)

**TRANSMISSION TEST**

<table>
<thead>
<tr>
<th>Signal</th>
<th>Yes</th>
<th>No</th>
<th>Time</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FINAL TEST REPORT

The following did not operate properly:

_____________________________________________________

_____________________________________________________

_____________________________________________________

_____________________________________________________

_____________________________________________________

**NOTIFICATION OF END OF TESTING**

Notify party responsible for the protected premises:

Name: ___________________________ Date: __________ Time: __________

Monitoring station:

Name: ___________________________ Date: __________ Time: __________

System restored to normal operation:

Date: __________ Time: __________

**Testing was performed in accordance with applicable NFPA standards.**

Name of inspector: ___________________________ Date: __________

Signature: ___________________________ Time: __________

Party responsible for the protected premises:

Date: __________

Signature: ___________________________ Time: __________

© 2010 National Fire Protection Association

NFPA 731 (p. 2 of 2)

A.4.7.2.2.1 A.4.14.3.1 Training should be based on the level of involvement with the system that the user will have. That level can be as simple as how to arm and disarm an intrusion detection system to as complex as setting how to set levels of access within an access control system. This training can be provided by, but is not limited to, one-to-one personal training, interactive video or CD-ROM, web-based distance learning, or user training manuals. This training needs to be ongoing, not only for new users of a premises security
system but as reinforcement for existing users. Training for all users should take place if the existing system changes due to a system enhancement or due to a tenant improvement.

A.4.7.2.2  A.4.14.3.2  This The documentation should contain, at a minimum, the names of the users trained, the date that the training was provided, and the scope of the training.
**A.6.1.5.3**
The portal locks can be bypassed during specific time periods of a day, based upon the access control system time schedule. When the portal locks are bypassed, the portal can automatically close but not lock.

**A.6.1.5.4**
Applicable codes and standards can include, but are not limited to, NFPA 101, *Life Safety Code*; NFPA 5000, *Building Construction and Safety Code*; NFPA 72, *National Fire Alarm and Signaling Code*; and amendments adopted by the AHJ. Based on the SVA of the protected premises, the designer might also wish to consider ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

**A.6.1.5.5**
The means of lock release detailed in 6.1.5.6 are not necessarily required for occupancies such as detention and correctional occupancies, psychiatric hospitals, or other occupancies where locked doors are permitted and egress or relocation is supervised by trained staff, provided staff has a means to release the lock and the AHJ approves such an installation.

**Statement**: The TC revises the Annex references for consistency and to correlate with FR# 6.

---

**A.7.2.3**
The quality of the image should not be impaired by the method used to provide vandal resistance. Suitable installation techniques could include the mounting and positioning of the camera so that, without compromising the requirements of Section 7.2, it is not readily accessible to a vandal. Information regarding SVA risk assessment procedures can be found in NFPA 730, *Guide for Premises Security Code*.

**Statement**: The TC changes risk assessment to SVA for consistency. The TC changes "Guide for" to "Code" as NFPA 730 is changed to enable visibility, adoptability and enforcement.

---

**A.7.4**
In addition to the manufacturer’s instructions, the choice of an enclosure should be based on application, environmental concerns, an SVA risk assessment, or the AHJ. An enclosure should be chosen that best protects the camera and lens combination from the ambient environment. Some considerations are indoor or outdoor location, temperature extremes, high humidity or condensing moisture, salt-water exposure, rain, snow, hazardous or volatile atmospheres, vandalism, and tampering. Each camera location should be assessed to determine which factors exist and the appropriate enclosure type and enclosure options chosen to best suit the needs of that location.

**Statement**: The TC changes risk assessment to SVA for consistency.
731- Log #FR11  
(A.9.3.4.4)

Final Action:

Submitter: Technical Committee Premises Security  
Recommendation: Text to read as follows:
A.9.3.4.4  The determination of the type of detection device to be used should be based on an SVA risk assessment for the facility. NFPA 730, Guide for Premises Security Code, can be used. Building designers should consider security through environmental design and should provide zones immediately around the facility to ensure security of the grounds and the safety of the personnel within.

Statement: The TC changes risk assessment to SVA for consistency. The TC changes "Guide for" to "Code" as NFPA 730 is changed to enable visibility, adoptability and enforcement.

731- Log #FR12  
(A.10.2.2)

Final Action:

Submitter: Technical Committee Premises Security  
Recommendation: Text to read as follows:
A.10.2.2  Temporary mitigating measures should be considered by the owner or responsible party during impairments based on an SVA assessment of the risk to the protected property or the occupants. Depending on the SVA risk assessment, the AHJ can be consulted. The recommendations from the consultation should be implemented for the period that the system is impaired.

Statement: The TC changes risk assessment to SVA for consistency.

731- Log #FR3  
(D.1.2.4)

Final Action:

Submitter: Technical Committee Premises Security  
Recommendation: Text to read as follows:

Statement: The TC updates the referenced standards to the most recent editions.
Submitter: Technical Committee Premises Security

Recommendation: Text to read as follows:

D.2 Informational References. The following documents or portions thereof are listed here as informational resources only.

They are not a part of the requirements of this document.


Statement: The TC updates the referenced standards to the most recent editions.