NFPA 731

Standard for the Installation of Electronic Premises Security Systems

2006 Edition

NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA DOCUMENTS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA DOCUMENTS

NFPA codes, standards, recommended practices, and guides, of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in its codes and standards.

The NFPA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making this document available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does the NFPA list, certify, test or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Documents

Users of NFPA codes, standards, recommended practices, and guides should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments. An official NFPA document at any point in time consists of the current edition of the document together with any Tentative Interim Amendments and any Errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of Tentative Interim Amendments or corrected through the issuance of Errata, consult appropriate NFPA publications such as the National Fire Codes® Subscription Service, visit the NFPA website at www.nfpa.org, or contact the NFPA at the address listed below.

Interpretations of NFPA Documents

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing Committee Projects shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights asserted in connection with any items which are mentioned in or are the subject of NFPA codes, standards, recommended practices, and guides, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on these documents. Users of these documents are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

NFPA adheres to applicable policies of the American National Standards Institute with respect to patents. For further information contact the NFPA at the address listed below.

Law and Regulations

Users of these documents should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the NFPA. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making this document available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to this document.

Use of NFPA documents for regulatory purposes should be accomplished through adoption by reference. The term “adoption by reference” means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA documents, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA codes, standards, recommended practices, and guides and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA documents during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101.

For more information about NFPA, visit the NFPA website at www.nfpa.org.

Copyright © 2005, National Fire Protection Association, All Rights Reserved

NFPA 731

Standard for the

Installation of Electronic Premises Security Systems

2006 Edition

This edition of NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* was prepared by the Technical Committee on Premises Security and acted on by NFPA at its June Association Technical Meeting held June 6–10, 2005, in Las Vegas, NV. It was issued by the Standards Council on July 29, 2005, with an effective date of August 18, 2005.

This edition of NFPA 731 was approved as an American National Standard on August 18, 2005.

Origin and Development of NFPA 731

The 2006 edition of NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* is the first edition of this standard. This standard was developed in parallel with NFPA 730, *Guide for Premises Security.* NFPA 731 provides details of how to install electronic premises security equipment. In addition to installation requirements, testing, inspection, and maintenance are addressed to provide a comprehensive document.

Technical Committee on Premises Security

Wayne D. Moore, *Chair*
Hughes Associates, Inc., RI [SE]

Raymond A. Grill, *Secretary*
The RJA Group, Inc., VA [SE]

Allan M. Apo, Insurance Services Office, Inc., NJ [I]
Chadwick Callaghan, Marriott International, Inc., DC [U]
Rep. American Society for Industrial Security
Louis Chavez, Underwriters Laboratories Inc., IL [RT]
Thomas L. Chronister, Oxnard Police Department, CA [E]
David S. Collins, The Preview Group, Inc., OH [SE]
Rep. American Institute of Architects
Jerry M. Cordasco, Compass Technologies, PA [M]
Wendell H. Couch, Six Continents Hotels, GA [U]
Rep. American Hotel & Lodging Association
Michael D. DeVore, State Farm Mutual Automobile Insurance Co., IL [U]
Rep. NFPA Industrial Fire Protection Section
John C. Fannin, III, SafePlace Corporation, DE [SE]
Rep. State of Delaware, Department of Safety and Homeland Security
Louis T. Fiore, L. T. Fiore, Inc., NJ [IM]
Rep. Professional Alarm Services Organizations of North America
Bruce Fraser, Tyco/SimplexGrinnell, MA [M]
Dale M. Gigandet, Pacom Systems Inc., FL [M]
Charles E. Hahl, The Protection Engineering Group, PLC, VA [SE]
Patrick D. Harris, Virginia Crime Prevention Association, VA [U]
Walter W. Jones, U.S. National Institute of Standards & Technology, MD [RT]
Stewart Kidd, Loss Prevention Consultancy, Ltd., United Kingdom [SE]
John M. Lombardi, Commercial Instruments & Alarm Systems, Inc., NY [IM]
Rep. Central Station Alarm Association
Tom G. Smith, Cox Systems Technology, OK [IM]
Rep. National Electrical Contractors Association
Bill H. Strother, Weingarten Realty Management Co., TX [U]
Rep. International Council of Shopping Centers
Michael Tierney, Builders Hardware Manufacturers Association, CT [M]
Mark A. Visbal, Security Industry Association, VA [M]
Raymond Walker, Town of Windsor, CT [E]

Alternates

Shane M. Clary, Bay Alarm Company, CA [IM]
(Alt. to J. M. Lombardi)
Kurt W. Collins, The RJA Group, Inc., IL [SE]
(Alt. to R. A. Grill)
Larry R. Dischert, Tyco/ADT Security Services, Inc., NJ [M]
(Alt. to M. A. Visbal)
Kevin J. Gainor, Tyco International, MA [M]
(Alt. to B. Fraser)
Mark M. Hankewycz, Gage-Babcock & Associates, Inc., VA [SE]
(Voting Alt. to Gage-Babcock Rep.)
Robert G. Harrington, Pyramid Management Group, Inc., NY [U]
(Alt. to B. H. Strother)
Gregory Kurasz, Virginia Crime Prevention Association, VA [U]
(Alt. to P. D. Harris)
Patrick M. Murphy, Marriott International, Inc., DC [U]
(Alt. to C. Callaghan)
Armando Porto, Metropolitan Transportation Authority, NY [U]
(Voting Alt.)
Steven A. Schmit, Underwriters Laboratories Inc., IL [RT]
(Alt. to L. Chavez)
Dean K. Wilson, Hughes Associates, Inc., PA [SE]
(Alt. to W. D. Moore)

Richard P. Bielen, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents on the overall security program for the protection of premises, people, property, and information specific to a particular occupancy. The Committee shall have responsibility for the installation of premises security systems.

Contents

NFPA 731

Standard for the

Installation of Electronic Premises Security Systems

2006 Edition

IMPORTANT NOTE: This NFPA document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notices and Disclaimers Concerning NFPA Documents." They can also be obtained on request from NFPA or viewed at www.nfpa.org/disclaimers.

NOTICE: An asterisk (*) following the number or letter designating a paragraph indicates that explanatory material on the paragraph can be found in Annex A.

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex D. Editorial changes to extracted material consist of revising references to an appropriate division in this document or the inclusion of the document number with the division number when the reference is to the original document. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

Information on referenced publications can be found in Chapter 2 and Annex D.

Chapter 1 Administration

1.1 Scope. This standard covers the application, location, installation, performance, testing, and maintenance of electronic premises security systems and their components.

1.2 Purpose.

1.2.1 The purpose of this standard is to define the means of signal initiation, transmission, notification, and annunciation; the levels of performance; and the reliability of electronic premises security systems.

1.2.2 This standard defines the features associated with these systems and also provides information necessary to modify or upgrade an existing system to meet the requirements of a particular application.

1.2.3 This standard establishes minimum required levels of performance, extent of redundancy, and quality of installation but does not establish the only methods by which these requirements are to be achieved.

1.2.4 This standard shall not be interpreted to require a level of premises security other than that required by the applicable codes and standards.

1.3 Application.

1.3.1 Electronic Premises Security Systems. Electronic premises security systems shall include one or more of the following system types:

(1) Intrusion detection systems
(2) Access control systems
(3) Video surveillance systems
(4) Asset protection systems
(5) Environmental detection systems
(6) Holdup and duress systems
(7) Integrated systems

1.3.2 Endorsement. Any reference or implied reference to a particular type of hardware is for the purpose of clarity and shall not be interpreted as an endorsement.

1.3.3 Technical Terms. The intent and meaning of the terms used in this standard shall be, unless otherwise defined herein, the same as those of NFPA 70, *National Electrical Code*.

1.3.4 Covered Locations.

1.3.4.1 Electronic Hardware Components. This standard applies to new installations of electronic premises security systems or their components installed for protection of building interiors, building perimeters, and surrounding property.

1.3.4.2 Other Hardware Components. This standard applies to nonelectronic building and physical security components where these items interface with, or become part of, an electronic premises security system.

1.3.4.3 Software. In this standard, software includes the system firmware.

1.3.5 Exclusions.

1.3.5.1 One- and Two-Family Dwellings. Electronic premises security systems installed in one- and two-family dwellings are not covered by this standard.

1.3.5.2 Information Technology Systems. The security of data or software in information technology or computer systems is not covered by this standard.

1.3.5.3 Portable Assets. The authorized removal of portable articles is not covered by this standard.

1.3.5.4 Transmission Methods. Transmission methods of off-premises communication networks and receipt of signals at monitoring stations are not covered by this standard.

1.3.5.5 Monitoring Stations. Monitoring stations that are receiving signals from electronic premises security systems and are not located at the protected property are not covered by this standard.

1.4 Retroactivity.

1.4.1 The provisions of this standard reflect situations and the state of the art at the time the standard was issued.

1.4.2 Unless otherwise noted, it is not intended that the provisions of this standard be applied to facilities, equipment, structures, or installations that were existing or approved for construction or installation prior to the effective date of this standard.

1.5 Equivalency.

1.5.1 A device or system having materials or forms that differ from those detailed in this standard shall be permitted to be examined and tested according to the intent of the standard and, if found equivalent, shall be approved.

1.5.2 Technical documentation shall be submitted to the authority having jurisdiction to demonstrate equivalency.

1.6 Units and Formulas.

1.6.1 Units. Metric units of measurement in this standard are in accordance with the modernized metric system known as the International System of Units (SI).

1.6.2 Primary and Equivalent Values. If a value for a measurement as given in this standard is followed by an equivalent value in other units, the first stated value shall be regarded as the requirement. A given equivalent value might be approximate.

1.6.3 Conversion Procedure. SI units have been converted by multiplying the quantity by the conversion factor and then rounding the result to the appropriate number of significant digits.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document.

2.2 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 70, *National Electrical Code®,* 2005 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2005 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2005 edition.

NFPA 780, *Standard for the Installation of Lightning Protection Systems,* 2004 edition.

2.3 Other Publications.

2.3.1 ANSI Publication. American National Standards Institute, Inc., 25 West 43rd Street, 4th Floor, New York, NY 10036.

ANSI S1.4-1983 (R 2001) with Amd. S1.4A-1985, *Specification for Sound Level Meters*, 2001.

2.3.2 SIA Publications. Security Industry Association, 635 Slaters Lane, Suite 110, Alexandria, VA 22314.

ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity,* 2000.

ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* 2000.

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

UL 294, *Standard for Access Control System Units,* 1999, revised 2004.

UL 365, *Standard for Police Station Connected Burglar Alarm Units and Systems,* 1997, revised 2001.

UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems,* 1999.

UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems,* 2000.

UL 636, *Standard for Holdup Alarm Units and Systems,* 1996, revised 2001.

UL 639, *Standard for Safety for Intrusion-Detection Units,* 1997, revised 2002.

UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems,* 1999, revised 2001.

UL 2044, *Standard for Commercial Closed Circuit Television Equipment,* 1997, revised 2004.

2.3.4 U.S. Government Publication. U.S. Government Printing Office, Washington, DC 20402.

Title 47, Code of Federal Regulations, Part 15, "Radio Frequency Devices."

2.3.5 Other Publication.

Merriam-Webster's Collegiate Dictionary, Merriam-Webster Inc., Springfield, MA, 2003.

2.4 References for Extracts in Mandatory Sections.

NFPA 72®, National Fire Alarm Code®, 2002 edition.

Chapter 3 Definitions

3.1* General. The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, shall be the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1* Approved. Acceptable to the authority having jurisdiction.

3.2.2* Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

3.2.4* Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

3.2.5 Shall. Indicates a mandatory requirement.

3.2.6 Should. Indicates a recommendation or that which is advised but not required.

3.2.7 Standard. A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions shall be located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard.

3.3 General Definitions.

3.3.1* Access Control. The monitoring or control of traffic through portals of a protected area by identifying the requestor and approving entrance or exit.

3.3.2* Active Lock. An electric locking device that holds a portal closed and cannot be opened for egress by normal operation of the door hardware.

3.3.3* Ancillary Functions. Monitored points that are not security points but are incorporated into an electronic premises security system or outputs that are not necessary to the function of the electronic premises security system.

3.3.4* Annunciator. A unit containing one or more indicator lamps, alphanumeric displays, computer monitor, or other equivalent means on which each indication provides status information about a circuit, condition, system, or location.

3.3.5* Closed Circuit Television (CCTV). A video system in which an analog or digital video signal travels from the camera to video monitoring stations at the protected premises.

3.3.6 Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [*72*, 2002]

3.3.7 Controller. A control unit used to provide the logic in an access control system.

3.3.8 Detection.

3.3.8.1 ***Intrusion Detection.*** The ability to detect the entry or attempted entry of a person or vehicle into a protected area.

3.3.8.2 ***Sound Detection.*** Recognition of an audio pattern indicative of unauthorized activity.

3.3.9 Device.

3.3.9.1 ***Initiating Device.*** A system component that originates transmission of a change-of-state condition.

3.3.9.1.1 ***Ambush Alarm Initiating Device.*** An initiating device or procedure that personnel authorized to disarm the intrusion system at a protected premises can use to transmit a signal indicating a forced disarming of an intrusion detection system.

3.3.9.1.2* ***Duress Alarm Initiating Device.*** An initiating device intended to enable a person at protected premises to indicate a hostile situation.

3.3.9.1.3* ***Holdup Alarm Initiating Device.*** An initiating device intended to enable an employee of a protected premises to transmit a signal indicating a robbery has transpired.

3.3.9.2 ***Signaling Device.*** A device that indicates an alarm or abnormal condition by means of audible, visual, or both methods, including sirens, bells, horns, and strobes.

3.3.10 Electronic Premises Security System. See 3.3.24.4.

3.3.11* False Alarm. Notification of an alarm condition when no evidence of the event that the alarm signal was designed to report is found.

3.3.12* Foil. An electrically conductive ribbon used for a sensing circuit.

3.3.13 Keypad. A device that is a type of human/machine interface (HMI) with numerical or function keys that can incorporate an annunciator or signaling device.

3.3.14* Monitoring Station. A facility that receives signals and has personnel in attendance at all times to respond to these signals.

3.3.15 Position Sensor. A device that indicates whether a portal is open or closed.

3.3.16 Protective Wiring.

3.3.16.1 ***Fine Wire Lacing.*** Bare, hand-drawn, solid copper wire not larger than 24 AWG or film-coated solid copper wire not larger than 26 AWG or the equivalent applied to a door or similar surface in continuous parallel strips.

3.3.16.2 ***Grooved Striping.*** Soft wooden half round dowels that are assembled to a surface in parallel runs of opposite polarity.

3.3.16.3 ***Open Wiring.*** A form of protective wiring used across skylights and in areas not subject to damage consisting of bare, hard-drawn solid copper wire not larger than 24 AWG that is arranged in two perpendicular banks of horizontal runs of opposite polarity at intervals not exceeding 102 mm (4 in.).

3.3.17* Reader. A device that allows an identification credential to be entered into an access control system.

3.3.18 Record of Completion. A document that acknowledges the features of installation, operation (performance), service, and equipment with representation by the property owner, system installer, system supplier, service organization, and the authority having jurisdiction. [*72*, 2002]

3.3.19 Safe. An iron, steel, or equivalent container that has its door(s) equipped with a combination lock.

3.3.20* Screens. A fully framed assembly of grooved-wood dowels or meshed screening that is intended to form a protective barrier over windows or on doors, and on which fine wire lacing is installed in parallel runs of opposite polarity at intervals not exceeding 102 mm (4 in.).

3.3.21 Security Personnel. Employees or contract service personnel charged with duties to aid in the protection at a protected premises.

3.3.22 Signals.

3.3.22.1* ***Alarm Signals.*** A signal indicating an unauthorized event at a protected premises.

3.3.22.2 ***Supervisory Signals.*** A signal indicating the need for action in connection with the supervision of guard tours, unverified exterior alarm, or environmental or other nonintrusion monitored point or system.

3.3.22.3 ***Trouble Signals.*** A signal indicating a fault in a monitored circuit or component.

3.3.23 Strain Relief. Cable termination that provides structural rigidity of conductors under conditions of flexure.

3.3.24 System.

3.3.24.1 ***Combination System.*** A system of multiple control units that work together to provide one integrated control.

3.3.24.2* ***Digital Imaging System (DIS).*** A video system in which a digital video signal travels from the camera and can be viewed by any authorized user at or away from the protected premises.

3.3.24.3 ***Duress Alarm System.***

3.3.24.3.1 ***Private Duress Alarm System.*** A system or portion thereof in which the action to activate the duress signal is known only to the person activating the device.

3.3.24.3.2 ***Public Duress Alarm System.*** A system or portion thereof in which the ability to activate a duress signal is available to any person at the protected premises.

3.3.24.4 ***Electronic Premises Security System.*** A system or portion of a combination system that consists of components and circuits arranged to monitor or control activity at or access to a protected premises.

3.3.24.5 ***Holdup Alarm System.***

3.3.24.5.1 ***Manual Holdup Alarm System.*** A system or portion thereof in which the initiation of a holdup signal depends solely on operation of manually operated hand or foot initiating devices installed within the working area.

3.3.24.5.2 ***Semiautomatic Holdup Alarm System.*** A system or portion thereof in which the initiation of a holdup signal does not depend solely on operation of manually operated hand or foot initiating devices installed within the working area.

3.3.24.6* ***Integrated System.*** A control unit that includes other types of systems in addition to the electronic premises security system.

3.3.24.7 ***Partition System.*** A part of one control unit that through software acts as a separate control unit.

3.3.25 Trap.

3.3.25.1* ***Ball Trap.*** A device consisting of two spring-tensioned balls that form a connector into which a flat metal clip that is attached to a conductor can be inserted to complete a circuit.

3.3.25.2 ***Barrier Bar Trap.*** A device consisting of a pressure-sensitive switch that is mounted onto one end of an adjustable bar that is installed across an opening.

3.3.25.3* ***Disconnecting Trap.*** A device intended to supervise the position of an air conditioner, small fan, fixed panel, or similar opening against movement in either direction with the use of a conductor or trip cord extended across the opening.

3.3.26* Vault. A room constructed of iron, steel, brick, concrete, stone, tile, or similar masonry units permanently built into or assembled on the premises and having an iron, steel, or equivalent door and frame with a combination lock.

Chapter 4 Fundamentals

4.1 Application.

4.1.1 This standard shall apply to new installations and provide the information necessary to modify or upgrade an existing system to meet the requirements for a particular type of system.

4.1.2 The provisions of Chapter 4 shall apply to Chapters 5 through 9.

4.1.3 When an electronic premises security system connects to fire alarm or other life safety systems, the requirements of other codes and standards shall be followed.

4.1.4 General.

4.1.4.1 The provisions of Chapter 4 shall cover the basic functions of an electronic premises security system.

4.1.4.2 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.

4.1.5 Equipment.

4.1.5.1 Where applicable nationally recognized standards exist, equipment constructed and installed in conformity with this standard shall be listed for the purpose for which it is used.

4.1.5.2 Compatibility. All electronic premises security system devices that receive their power from the initiating device circuit or signaling line circuit of an electronic premises security control unit shall be listed for use with the control unit.

4.1.5.3 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.

4.1.6* System Design. 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.

4.1.6.1 The system designer shall be identified on the system design documents.

4.1.6.2 Evidence of qualifications shall be provided when requested by the authority having jurisdiction.

4.1.6.3 Qualified personnel shall include, but not be limited to, the following:

(1) Equipment manufacturer trained and certified personnel
(2) Personnel licensed and certified by state or local authority
(3) Personnel certified by an accreditation program acceptable to the authority having jurisdiction (AHJ)

4.1.7* System Installation.

4.1.7.1 Installation personnel shall be supervised by persons who are qualified and experienced in the installation, inspection, and testing of electronic premises security systems.

4.1.7.2 Qualified personnel shall include, but not be limited to, the following:

(1) Equipment manufacturer trained and certified personnel
(2) Personnel licensed or certified by federal, state, or local authority
(3) Personnel certified by an accreditation 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

4.2 Power Supplies.

4.2.1 Scope. The provisions of this section shall apply to power supplies used for electronic premises security systems.

4.2.2 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 this subsection.

4.2.3 Power Sources.

4.2.3.1 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

4.2.3.2 When required by 4.2.3.1, all power supplies and subpanels shall meet the requirements of 4.2.3.1.

4.2.3.3* 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.

4.2.3.4 Where direct current (dc) voltages are employed, they shall be limited to no more than 350 volts above earth ground.

4.2.4 Primary Supply.

4.2.4.1 Dedicated Branch Circuit.

4.2.4.1.1 One of the following dedicated branch circuits shall supply primary power:

(1) Commercial light and power
(2) An engine-driven generator or equivalent in accordance with 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 4.2.9, where a person specifically trained in its operation is on duty at all times

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

4.2.4.2 Mechanical Protection.

4.2.4.2.1 Circuit disconnecting means shall have a blue marking, shall be accessible only to authorized personnel, and shall be identified as "PREMISES SECURITY CIRCUIT."

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

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

4.2.4.4 Transient Voltage Surge Protection. 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 sub-panels
(3) Microprocessor-based annunciators
(4) Other microprocessor-based equipment

4.2.4.5 Circuit Breakers and Engine Stops. 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.

4.2.5 Light and Power Service.

4.2.5.1 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.

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

4.2.5.3 For an integrated system, the secondary supply capacity required by 4.2.3.1 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.

4.2.5.4 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 4.2.8
(2) A dedicated branch circuit of an automatic-starting engine-driven generator arranged in accordance with 4.2.9 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

4.2.6 Capacity.

4.2.6.1* 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 24 hours and, at the end of that period, shall be capable of operating all alarm sounding devices for 15 minutes, where required.

4.2.6.2 Secondary Power Operation.

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

4.2.6.2.2 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.

4.2.7 Continuity of Power Supplies.

4.2.7.1 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.

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

4.2.7.2.1 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.

4.2.7.2.2 Where a UPS is employed in 4.2.7.2.1, 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.

4.2.8 Storage Batteries.

4.2.8.1 Marking. Batteries shall be permanently marked with the month and year of manufacture.

4.2.8.2 Replacement.

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

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

4.2.8.3 Location. Storage batteries shall be located so that the premises security equipment, including overcurrent devices, are not adversely affected by battery gases and shall conform to the requirements of NFPA 70, *National Electrical Code*, Article 480.

4.2.8.3.1 Cells shall be insulated against grounds and crosses and shall be mounted securely in such a manner so as not to be subject to mechanical injury.

4.2.8.3.2 Racks shall be protected against deterioration.

4.2.8.3.3 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.

4.2.8.3.4 In-line overcurrent protection shall be between the secondary power supply batteries and the secondary power supply.

4.2.8.4 Battery Charging.

4.2.8.4.1 A means shall be provided to automatically maintain the battery fully charged under all conditions of normal operation.

4.2.8.4.2 A means shall be provided to recharge batteries within 24 hours after fully charged batteries have been subject to discharge.

4.2.8.4.3 Upon attaining a fully charged condition, the charge rate shall not result in battery damage.

4.2.8.5 Overcurrent Protection.

4.2.8.5.1 The batteries shall be protected against excessive load current by overcurrent devices.

4.2.8.5.2 The batteries shall be protected from excessive charging current by overcurrent devices or by automatic current-limiting design of the charging source.

4.2.8.6 Charger Supervision. 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.

4.2.9 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*.

4.3 System Functions.

4.3.1 Electronic Premises Security System.

4.3.1.1 Electronic premises security system functions shall be permitted to be performed automatically.

4.3.1.2 The performance of electronic premises security system functions shall not interfere with power for fire alarms, lighting, or operation of elevators or other building control systems.

4.3.1.3 The performance of electronic premises security system functions shall not preclude the combination of other services requiring monitoring of operations.

4.3.2 Time Delay. The time delays shall be determined by other sections of this standard.

4.3.3 Distinctive Signals. Electronic premises security system alarms, supervisory signals, and trouble signals shall be distinctively and descriptively annunciated.

4.4 Performance and Limitations.

4.4.1 Voltage, Temperature, and Humidity Variation. 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)

4.4.2 Damp, Wet, or Exterior Environments. Equipment intended for use in damp, wet, or exterior environments shall be listed for its use.

4.5 Installation and Design.

4.5.1 AHJ Approval. All systems shall be installed in accordance with the specifications and standards approved by the AHJ.

4.5.2* Site Inspection. The site shall be inspected for environmental factors that affect the operation of the electronic premises security system.

4.5.3 Environment. The devices installed shall perform their intended functions in the environmental conditions at the protected premises.

4.5.4 Equipment Mounting.

4.5.4.1 Devices, appliances, and control units shall be located and mounted so that accidental operation or failure is not caused by vibration or jarring.

4.5.4.2 Unless otherwise permitted by the manufacturer, control units, power supplies, and batteries shall be mounted in the vertical, upright position.

4.5.5 Manual Resetting. 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.

4.5.6 Equipment Location.

4.5.6.1 Equipment shall be installed in locations where conditions do not exceed the voltage, temperature, and humidity limits specified in 4.4.1 unless listed for the application.

4.5.6.2 Interconnecting Control Units.

4.5.6.2.1 Control units, subcontrols, and devices that are used to interconnect the control unit to protection devices shall be located within the area being protected by the system.

4.5.6.2.2 If the enclosures for such equipment are not located in such an area, the enclosures shall be protected by one of the following methods:

(1) Continuously under the notice of assigned security personnel
(2) Located in an area that is accessible only to authorized personnel
(3) Supervised to annunciate tampering

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

4.5.7 Protection. 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*, Article 800.

4.5.8 Wiring.

4.5.8.1 General.

4.5.8.1.1 The installation of all wiring, cable, and equipment shall be performed in a workman-like manner in accordance with NFPA 70, *National Electrical Code*, and specifically with Article 725 or 800, where applicable.

4.5.8.1.2 Optical fiber cables shall be protected against mechanical injury in accordance with NFPA 70, *National Electrical Code*, Article 770.

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

4.5.8.3* Unless specifically allowed by the manufacturer's wiring specifications, low voltage electronic premises security system wiring shall be spaced at least 5.08 cm (2 in.) from conductors of any light and power circuits, unless one of the circuits is in metal raceway.

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

4.5.8.5 Termination.

4.5.8.5.1 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.

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

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

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

4.5.8.5.5 Conductors shall be of the same size and composition.

4.5.8.5.6 Terminals shall be marked or colored coded where necessary to indicate the proper connections.

4.5.8.6* 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*, Articles 725 and 800.

4.5.8.7 Circuit Identification.

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

4.5.8.7.2 Circuit identification shall be at all field terminations.

4.5.8.7.3 Circuit identification shall not be visible to the public.

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

4.5.8.9 Service Loop Metallic Conductors.

4.5.8.9.1 A minimum 15.24 cm (6 in.) service loop shall be at control panels and enclosures used for wiring terminations.

4.5.8.9.2 A minimum 15.24 cm (6 in.) service loop shall be at field terminations.

4.5.8.9.3 Service loops shall be mechanically protected.

4.5.8.10 Service Loop Optical Fiber Cable.

4.5.8.10.1 A service loop shall be at control panels and enclosures used for terminations.

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

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

4.5.8.10.2 A service loop shall be at field terminations.

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

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

4.5.8.10.3 Service loops shall be mechanically protected.

4.5.9* Low-Powered Radio (Wireless) Systems.

4.5.9.1* Listing Requirements. Compliance with 4.5.9 shall require the use of low-powered radio equipment specifically listed for the purpose.

4.5.9.2 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/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) Catastrophic (open or short) 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 resound at least once every 4 hours.
(7) Any mode of failure of a primary battery in a low-powered radio transmitter shall not affect any other low-power radio transmitter.

4.5.9.3 Alarm Signals.

4.5.9.3.1* When actuated, each low-powered radio transmitter shall automatically transmit a signal indicating the cause of the activation.

4.5.9.3.2 Each low-powered radio transmitter shall automatically repeat alarm transmissions at intervals not exceeding 60 seconds until the initiating device is returned to its nonalarm condition.

4.5.9.3.3 Fire alarm signals shall have priority over all other signals, including those from electronic premises security systems.

4.5.9.3.4 The maximum allowable response delay from activation of an initiating device to receipt and display by the receiver/control unit shall be 90 seconds.

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

4.5.9.4 Monitoring for Integrity.

4.5.9.4.1* 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.

4.5.9.4.2 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

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

4.5.9.4.4 The periodic transmission required to comply with 4.5.9.4.2 from a low-powered radio transmitter shall ensure successful alarm transmission capability.

4.5.9.4.5 Removal of a low-powered 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.

4.5.9.4.5.1 The requirement of 4.5.9.4.5 shall not apply to dwelling unit electronic premises security systems.

4.5.9.4.6 Trouble Indication.

4.5.9.4.6.1 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.

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

4.5.9.5 Output Signals from Receiver/Control. 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 4.5.9.2.
(2) All supervision requirements of Chapter 4 or 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.

4.5.10 Grounding.

4.5.10.1 All grounding shall be in accordance with NFPA 70, *National Electrical Code*, Articles 250 and 800.

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

4.5.10.3 All other circuits shall test free of grounds.

4.5.11 Zoning and Annunciation.

4.5.11.1* General. 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.

4.5.11.2 Visible Zone Indication.

4.5.11.2.1* 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.

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

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

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

4.5.12 Testing. All electronic premises security systems shall be maintained and tested in accordance with Chapter 9.

4.5.13 Software Control.

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

4.5.13.2 A record of installed software version numbers shall be maintained at the location of the electronic premises security system.

4.5.13.3* All software shall be protected from unauthorized changes.

4.5.13.4 All changes shall be tested in accordance with Chapter 9.

4.6 System Requirements.

4.6.1 Electronic Premises Security Control Units.

4.6.1.1 General.

4.6.1.1.1 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.

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

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

4.6.1.2 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 be comprised of a primary power supply and a secondary power supply that shall meet the same requirements as those of 4.2.3 through 4.2.8.

4.6.1.3 When required, the method of interconnection of control units shall meet the monitoring requirements of Chapter 5, comply with NFPA 70, *National Electrical Code*, Articles 725 and 800, 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

4.6.1.4 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.

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

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

4.6.2 Combination Systems.

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

4.6.2.2 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.

4.6.3 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.

4.7 Documentation.

4.7.1 Approval and Acceptance.

4.7.1.1 The AHJ shall be notified prior to installation.

4.7.1.1.1 Notification of alteration of equipment or wiring shall be provided to the AHJ, if requested.

4.7.1.1.2 At the AHJ's request, complete information regarding the system or system alterations, including specifications and battery calculations, shall be provided.

4.7.1.2 Before requesting final approval of the installation, if required by the AHJ, the installing contractor shall furnish a written statement stating that the system has been installed in accordance with the specifications tested in accordance with the manufacturer's specifications and the appropriate NFPA requirements.

4.7.2 Documentation and User Training.

4.7.2.1* Documentation. Every system shall include the following documentation, which shall be delivered to the owner or the responsible party upon final acceptance of the system:

(1) *Owner's manual and installation instructions covering all system equipment
(2) User's instructions
(3) *Electronic Premises Security Record of Completion form completed by the installer of the system
(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

4.7.2.2 Training.

4.7.2.2.1* The owner or responsible party shall arrange for an appropriate level of training of the system users.

4.7.2.2.2* The user training shall be documented and maintained for 1 year, with the system documentation made available to the AHJ upon request.

4.8 Central Station Electronic Premises Security Systems.

4.8.1 If required, it shall be conspicuously indicated by the prime contractor that the electronic premises security system providing service at a protected premises complies with all applicable requirements of this standard by providing documentation as specified in 4.8.2.1.

4.8.2 The installed system shall be certificated.

4.8.2.1 Central station electronic premises security systems providing service that complies with all requirements of this standard shall be certificated by the organization that has listed the prime contractor, and a document attesting to this certification shall be located on or near the premises security system control unit or, where no control unit exists, on or near an electronic premises security system component.

4.8.2.2 A central repository of issued certification documents, accessible to the AHJ, shall be maintained by the organization that has listed the central station.

Chapter 5 Intrusion Detection Systems

5.1 General.

5.1.1 Monitoring Integrity of Conductors.

5.1.1.1 All means of interconnecting wiring connections between a control unit, keypads, power supplies, and accessories to the control unit shall be monitored for the integrity of the interconnecting conductors or equivalent path so that the occurrence of a single open or a single ground-fault condition in the installation conductors or other signaling channels and their restoration to normal shall be automatically indicated within 90 seconds.

5.1.1.2 Wiring to all initiating devices of an intrusion detection system shall be monitored for integrity so that the presence of an off-normal condition is automatically indicated to the user upon arming of the system.

5.1.1.3 When the system is armed, wiring to all initiating devices shall be monitored for integrity, so that the occurrence of a single open, a single ground-fault condition, or a wire-to-wire short shall be indicated at the control unit.

5.1.1.4 Interconnecting wiring of a stationary computer and the computer's keyboard, video monitor, mouse-type device, or touch screen need not be supervised, when the interconnecting wiring is as follows:

(1) Does not exceed 2.4 m (8 ft) in length.
(2) Is a listed computer/data processing cable as permitted by NFPA 70, *National Electrical Code*.
(3) Failure of the wiring does not cause the failure of the required system functions not initiated from the keyboard, mouse, or touch screen.

5.1.1.5 A fault on wiring to initiating devices shall not restore or clear an unacknowledged alarm signal at the control unit.

5.1.2 Reserved.

5.1.3 Entry/Exit Delay.

5.1.3.1 A single entry delay circuit shall be used on a system, subsystem, or partition.

5.1.3.2 A delay circuit that allows entry into a protected premises shall be limited to only those initiating devices, such as door contacts installed on entry doors and interior sensors, that must be bypassed to allow access to the mechanism that is used to place the system in a disarmed state.

5.1.3.3 The maximum interval of time between the opening of an entry door and reaching the mechanism that is used to disarm the system shall be no greater than one-half of the entry delay time programmed for the system.

5.1.3.4 The exit delay shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, Section 4.2.2.

5.1.3.5 The entry/exit delay time shall not exceed 240 seconds.

5.1.3.6 The entry/exit delay shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, Section 4.2.3.

5.1.4 Installation Requirements.

5.1.4.1 Devices shall be installed as per the manufacturer's instructions.

5.1.4.2 Coverage and spacing of devices shall be based upon the intended threat as specified by the designer in consultation with the end user.

5.2 Exterior Detection Systems.

5.2.1 Physical Verification.

5.2.1.1 Signals from exterior detection devices shall not be retransmitted to the AHJ unless physical verification of an intrusion is made.

5.2.1.2 Physical verification shall be made by one of the following:

(1) On-site verification
(2) Video verification

5.2.2 Signals transmitted to an off-site monitoring station shall be a supervisory signal.

5.2.3 When activated, exterior detection devices shall annunciate at the protected property and transmit a supervisory signal for verification.

5.2.4 Exterior Space Detection.

5.2.4.1 Photo Electric Cell (PEC).

5.2.4.1.1 PEC units shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.4.1.2 An alarm signal shall be initiated when a minimum of two of the following parallel units mounted on the same vertical plane are activated:

(1)*Two PEC units
(2) One PEC unit and one unit of another technology as described in this standard

5.2.4.2 Motion Detection.

5.2.4.2.1 Motion detection units shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.4.2.2 Passive infrared (PIR) units shall meet the requirements of ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity*.

5.2.4.3 Exterior Structural Detectors.

5.2.4.3.1 Exterior structural detectors shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, and UL 639, *Standard for Safety for Intrusion-Detection Units*, where applicable.

5.2.4.3.2 Exterior structural detectors shall include the following:

(1) Audio
(2) Contacts
(3) Fiber optic
(4) Protective cabling
(5) Proximity
(6) Shock sensors
(7) Stress sensors

5.2.4.4 Exterior Buried Detectors.

5.2.4.4.1 Exterior buried detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units*, where applicable.

5.2.4.4.2 Exterior buried detectors shall include the following types:

(1) Electromagnetic
(2) Fiber optic
(3) Leaky coaxial
(4) Seismic

5.3 Interior Detection Systems.

5.3.1 Interior detection devices shall be installed in accordance with UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*.

5.3.2 When activated, interior protection devices shall annunciate at the protected property and transmit an alarm signal.

5.3.3 Interior Perimeter Detection.

5.3.3.1 Doors, Windows, and Other Openings.

5.3.3.1.1 Contacts. Contacts shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*.

5.3.3.1.2 Protective Wiring.

5.3.3.1.2.1 Protective wiring shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems,* or UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems,* as applicable.

5.3.3.1.2.2 Protective wiring shall include the following:

(1) Grooved striping
(2) Lacing
(3) Open wiring
(4) Screens, including wood doweling and mesh type

5.3.3.1.3 Foil. Foil shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems.*

5.3.3.1.4 Traps.

5.3.3.1.4.1 Traps shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems.*

5.3.3.1.4.2 Traps shall include the following types:

(1) Ball
(2) Barrier bar
(3) Disconnecting

5.3.3.1.5 Shock (Vibration) Sensors. Shock sensors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.3.1.6 Glass Break Sensors.

5.3.3.1.6.1 Glass break sensors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.6.2 Glass break sensors shall include the following types:

(1) Shock
(2) Audio

5.3.3.1.7 Sound Detectors. Sound detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.8 Photo Electric Cell (PEC). PEC units shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.3.1.9 Motion Detection.

5.3.3.1.9.1 Motion detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.3.1.9.2 Motion detectors shall be used only in an environment and for an opening or area that is suitable.

5.3.3.1.9.3 Motion detectors shall include the following:

(1) Two or more technologies
(2) Microwave
(3) Passive infrared (PIR)

5.3.3.1.10 Video Motion Detection (VMD). When activated, video motion detectors shall annunciate at the protected premises and display the captured image.

5.3.4 Walls.

5.3.4.1 Protective Wiring.

5.3.4.1.1 Protective wiring shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.4.1.2 Protective wiring shall include the following:

(1) Fine wire lacing
(2) Grooved striping

5.3.4.2 Shock (Vibration) Sensors. Shock sensors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.4.3 Sound Detectors. Sound detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.4.4 Photo Electric Cell (PEC). PEC units shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.4.5 Motion Detection.

5.3.4.5.1 Motion detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.4.5.2 Motion detectors shall be used only in an environment and for an opening that is suitable.

5.3.4.5.3 Motion detectors shall include the following:

(1) Two or more technologies
(2) Microwave
(3) Passive infrared (PIR)

5.3.4.6 Video Motion Detection (VMD). When activated, video motion detectors shall annunciate at the protected premises and display the captured image.

5.3.5 Interior Space Protection.

5.3.5.1 For the protection of interior doors and openings that make up the boundary of an interior protected space, devices shall be installed in accordance with UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems.*

5.3.5.2 Pressure-Sensitive Devices.

5.3.5.2.1 Pressure-sensitive devices shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems,* or UL 639, *Standard for Safety for Intrusion-Detection Units,* as applicable.

5.3.5.2.2 Pressure-sensitive devices shall include the following:

(1) Floor mats
(2) Stair treads
(3) Stress sensors

5.3.5.3 Photo Electric Cell (PEC). PEC units shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.5.4 Motion Detection.

5.3.5.4.1 Motion detectors shall be listed in accordance with UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.3.5.4.2 Motion detectors shall be used only in an environment and for a space that is suitable.

5.3.5.4.3 Motion detectors shall include the following:

(1) Two or more technologies
(2) Microwave
(3) Passive infrared (PIR)

5.3.5.5 Video Motion Detection (VMD). When activated, video motion detectors shall annunciate at the protected premises and display the captured image.

5.4 Vaults and Safes.

5.4.1 Vaults.

5.4.1.1 Vault detection devices shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems,* and UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.4.1.2 Vault detection devices shall be installed in accordance with UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems.*

5.4.1.3 Vault detection shall include one or more of the following components:

(1) Contacts
(2) Embedded cable
(3) Foil lining
(4)*Heat detection
(5) Shock
(6)*Smoke detection
(7) Sound

5.4.2 Safes.

5.4.2.1 Safe detection devices shall be listed in accordance with UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems,* and UL 639, *Standard for Safety for Intrusion-Detection Units.*

5.4.2.2 Safe detection devices shall be installed in accordance with UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems.*

5.4.2.3 Safe detection shall include one or more of the following devices:

(1) Contacts
(2) Capacitance
(3) Foil lining
(4) Shock

5.4.3 Automatic Teller Machines.

5.4.3.1 Protection of automatic teller machines (ATMs) shall be the same as for safes, and the requirements of 5.3.2 shall be met.

5.4.3.2 Sound detection shall be listed for this application.

5.4.4 Secure Containers.

5.4.4.1 Protection of secure containers shall be the same as for safes, and the requirements of 5.3.2 shall be met.

5.4.4.2 Sound detection shall be listed for this application.

Chapter 6 Electronic Access Control Systems

6.1 Fundamentals. This section shall apply to physical electronic access control systems only.

6.1.1 Equipment. Electronic access control equipment shall be listed in accordance with UL 294, *Standard for Access Control System Units.*

6.1.2* Portal. The system shall be designed to control the unauthorized access of people, vehicles, and/or property through a portal as prescribed by the AHJ.

6.1.3* Reader.

6.1.3.1* Readers shall be mounted in accordance with adopted local codes and the requirements of the AHJ.

6.1.3.2 When the portal is a door, readers shall be mounted on the latch side.

6.1.3.3* Clearance between the reader and the portal shall be provided for the portal action appropriate for its application.

6.1.3.4 Access to the readers shall not be obstructed when manual presentation is required.

6.1.3.5 When manual presentation of access credentials is required for a vehicle, the reader shall be readily accessible from the operator's position of vehicles common to the site.

6.1.3.6 All readers shall provide a visual or audible indication that the credential has been recognized.

6.1.3.7* The maximum interval of time between the recognition of a valid credential and the unlocking of a portal shall not exceed 10 seconds.

6.1.4 Locking Systems. Access control systems shall utilize electric locking systems to control the use of portals.

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

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

6.1.4.3* Portals shall automatically close and lock when the portal is supervised by the access control system.

6.1.4.4* Where 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.

6.1.4.5 When a portal is a required means of egress and is provided with an active lock, a manual means, independent of the access control system, shall be provided that directly releases the active lock.

6.1.4.5.1* The manual means of release required for emergency egress portals in 6.1.4.5 shall not be required if approved by the AHJ.

6.1.5 Position Sensor.

6.1.5.1* A position sensor shall be required on all controlled portals.

6.1.5.2* A position sensor shall monitor the position of the portal for held-open or forced-open conditions.

6.1.5.3 The position sensor shall be mounted such that no portion of the portal can be opened greater than 15.24 cm (6 in.) before activating the sensor.

6.1.5.4 Position sensors shall be monitored as applicable by the head end controller or an integrated intrusion detection system so as to notify the system users of an event.

6.1.6* Portal Egress.

6.1.6.1 Free Egress.

6.1.6.1.1 Free egress shall employ the use of a request-to-exit (RTE) device.

6.1.6.1.2* When the RTE controls the portal lock, the lock shall open on loss of power.

6.1.6.1.3 When activated, RTE devices shall prevent the position sensor from reporting a forced-open alarm.

6.1.6.1.4 The RTE shall be either manual or automatic.

6.1.6.1.4.1 Manual.

(A) The RTE device shall not require any special instruction or knowledge to use.

(B) If a manual RTE device is used as a fail-safe for an automatic RTE device, it shall be installed so as to directly release the locking mechanism.

6.1.6.1.4.2 Automatic.

(A) If the RTE device is a motion detector, it shall be listed for its purpose.

(B) When automatic RTE devices are used to unlock portals, they shall be installed so that only intentional requests are executed.

6.1.6.2* Controlled Egress.

6.1.6.2.1 Controlled egress shall require the use of access credentials to be presented to a reader that is installed on the secured side of the portal in accordance with 6.1.3.

6.1.6.2.2* Active locks used for controlled egress shall meet the requirements of 6.1.4.5.

6.1.7 Controllers.

6.1.7.1 A controller shall be listed for its purpose.

6.1.7.2 A controller shall be installed per manufacturer's instructions.

6.1.7.3 A controller shall be installed in a space that protects it from damage, tampering, and access by unauthorized personnel.

6.1.8 Power Supplies.

6.1.8.1 Power supplies shall meet the requirements of Section 4.2.

6.1.8.2* Power supplies shall be sized based upon the application and manufacturer's requirements.

6.1.8.3 The voltage and current of the power supply shall be the same as required by the associated field devices.

6.1.8.4 Power supplies shall be installed in a space that protects them from damage, tampering, and access by unauthorized personnel.

6.2 Administration Tools/Interface.

6.2.1* The configuration of the system operating parameters shall be done in accordance with the facility requirements and subject to the approval of the AHJ.

6.2.2 All system operating parameters shall be protected from unauthorized changes.

6.2.3 Ancillary functions shall not interfere with the security and life safety–related functions.

6.2.4 Interconnections of components of an access control system shall be verified for compatibility.

6.3* Network Interface Device. In network interface device (NID) configurations, the level of encryption shall comply with the applicable level prescribed by the AHJ.

Chapter 7 Video Surveillance Systems

7.1 General.

7.1.1 This section shall cover the installation requirements for closed circuit television (CCTV) systems and analog and digital imaging systems (DIS).

7.1.2 The application and use of these systems shall be based on the requirements of AHJ, and the installer shall ensure that the final image meets the design requirements.

7.1.3 The system shall be designed to provide positive visual identification of a person, object, or scene as prescribed by the AHJ. *(See Annex B.)*

7.2 Cameras. Camera selection and location shall be based upon the requirements of the AHJ. *(See Annex C.)*

7.2.1 All cameras shall be listed for the purpose.

7.2.2 All cameras shall be installed as per the manufacturer's instructions.

7.2.3* The level of vandal resistance is determined by a risk assessment or the requirements of the AHJ.

7.2.4 In the absence of a risk assessment or AHJ requirement, cameras shall be installed so that the image cannot be impaired by vandalism.

7.2.5 In addition to the requirements of Chapter 4, cameras shall be installed so that the following environmental conditions do not affect their operation:

(1)*Icing
(2)*Sunlight angles
(3)*Temperature extremes
(4)*Wind loading
(5)*Rain

7.2.6 Backlighting.

7.2.6.1* The camera field of view shall not have bright illumination behind the main subject.

7.2.6.2* When the backlighting conditions in 7.2.6.1 cannot be met or the scenes have extreme contrast, high dynamic range or backlight compensation cameras shall be used.

7.3* Low-Level Lighting Conditions. Low-level lighting conditions of 10 lux or less within the field of view shall have special provisions to provide an image that meets the requirements of 7.1.3.

7.4* Enclosures. When enclosures are used, they shall be installed as per the manufacturer's instructions.

7.4.1 Physical Dimensions. The correct size enclosure shall be selected based on the dimensions of the camera/lens package and any other required equipment, such as connectors, other electronic devices, or transformers.

7.4.2 Listed. Enclosures shall be listed in accordance with UL 2044, *Standard for Commercial Closed Circuit Television Equipment.*

7.4.3 Tamper Resistance for Enclosures.

7.4.3.1 The level of tamper resistance shall be determined by a risk assessment or the requirements of the AHJ.

7.4.3.2 In the absence of a risk assessment or AHJ requirement, hardware shall be installed so that it cannot be removed without the use of hand tools.

7.5* General Hardware and Mounts. Mounting brackets shall be listed in accordance with UL 2044, *Standard for Commercial Closed Circuit Television Equipment.*

7.5.1 Anchoring.

7.5.1.1 Anchoring shall be rated for the load and mounting surface.

7.5.1.2 All anchoring sets shall be installed per manufacturers' instructions and be appropriate for the surface to which they are mounted.

7.5.1.3 All manufacturers' torque specifications shall be adhered to as applicable and be appropriate for the surface to which the anchoring sets are mounted.

7.5.2 Mounts. Mounts shall be rated for the weight, external weight (i.e., snow or rain), twist, and wind loading of the equipment used.

7.5.3 Mounting Bolts. Mounting bolts and hardware shall be tightened in accordance with 7.5.1.3.

7.5.4* Tamper Resistance for General Hardware and Mounts.

7.5.4.1 The level of tamper resistance shall be determined by a risk assessment or the requirements of the AHJ.

7.5.4.2 In the absence of a risk assessment or AHJ requirement, hardware shall be installed so that it cannot be removed without the use of hand tools.

7.6 Lens. Lenses shall be selected to provide the proper field of view and image size as required in 7.1.3.

7.7 Physical Conductors.

7.7.1* All cabling and wiring shall be installed in accordance with the requirements of 4.5.8.

7.7.2 Coaxial Cable.

7.7.2.1 Cable Specifications.

7.7.2.1.1* Coaxial cable shall have a jacket appropriate for the environment and shall be compliant with local codes.

7.7.2.1.2 The coaxial cable shall have a dielectric impedance of 75 ohms.

7.7.2.1.3 The shield of the coaxial cable shall be braided, 100 percent copper material with an efficiency rating (ER) of 95 percent or better, or reverse foil over copper braid with a 100 percent ER.

7.7.2.1.3.1 In installations where the coaxial cable flexes, such as pole to pole, a stranded center core shall be used.

7.7.2.1.3.2 In installations where the coaxial cable is fixed, such as inside raceway, a solid center core shall be used.

7.7.2.1.4 The center core shall be 100 percent copper with an outer diameter that matches the inner diameter of the center tit of the bayonet nut connector (BNC) that is to be installed.

7.7.2.2 Coaxial Cable Distances. Coaxial cable shall not be installed beyond the manufacturer's rated distances.

7.7.2.3 Coaxial Connections.

7.7.2.3.1 All connections shall be made with three-piece crimp BNC connectors.

7.7.2.3.2* The installer shall possess and understand the use of tools necessary to ensure proper cable stripping and crimping of three-piece BNC connectors.

7.7.2.3.3 The installer shall ensure that the inner diameter of the center tit of the connector matches the outer diameter of the center core of the cable.

7.7.2.3.4 Any discrepancies shall be corrected prior to the installation of such connectors.

7.7.2.3.5 The installer shall ensure that proper male to female, male to male, and female to female inline barrel connectors are used at all splice points.

7.7.3 Unshielded Twisted Pair. Unshielded twisted pair wire shall be installed in accordance with 4.5.8.

7.7.4 Fiber Optics. Fiber optic cable shall be installed in accordance with 4.5.8.

7.8* Applications of Conductors.

7.8.1* Control Wiring. All control wiring shall be sized to deliver the manufacturer's optimum operating voltage from the power supply or controller to the device being driven.

7.8.2 Power Cabling. Minimum size of power cabling shall be in accordance with NFPA 70, *National Electrical Code.*

7.8.3 Video Signal Transmission.

7.8.3.1* For nonamplified coaxial cable applications, distances shall not exceed those listed in Table 7.8.3.1.

Table 7.8.3.1 Coaxial Cable

Cable Type	Cable Distances	
	m	ft
RG-59	304.8	1000
RG-6	457.2	1500
RG-11	609.6	2000

7.8.3.2 Unshielded Twisted Pair (UTP). When UTP is used for video signal transmission, the maximum distance shall not exceed the manufacturer's instructions.

7.8.3.3 Fiber Optic (FO) Cable. When FO is used for video signal transmission, the maximum distance shall not exceed the manufacturer's instructions.

7.9* Radio Frequency (RF). (Reserved)

Chapter 8 Holdup, Duress, and Ambush Systems

8.1 General.

8.1.1 Construction.

8.1.1.1 The construction of holdup alarm initiating devices shall be listed in accordance with UL 636, *Standard for Holdup Alarm Units and Systems.*

8.1.1.2 The construction of duress alarm initiating devices shall be listed in accordance with UL 636, *Standard for Holdup Alarm Units and Systems.*

8.1.1.3 The construction of ambush alarm initiating devices shall be listed in accordance with UL 365, *Standard for Police Station Connected Burglar Alarm Units and Systems.*

8.1.2 Installation.

8.1.2.1 Systems that utilize wiring or low-powered radio frequency to connect initiating, annunciating, and remote control devices shall comply with Chapter 4.

8.1.2.2 The means of interconnecting wiring connections between initiating, annunciating, and remote control devices shall be supervised so that the occurrence of a single open or single ground-fault condition in the installation wiring and their restoration to normal shall be indicated within 200 seconds.

8.1.2.3 Initiating devices shall be located in such a manner to prevent unintentional operation by employees, janitors, cleaners, and others with access to the equipment.

8.1.2.4 Initiating devices shall be mounted in such a manner to prevent unintentional operation by jarring, vibration, falling objects, and similar causes.

8.1.2.5* Portable initiating devices shall require positive, intentional action to initiate an alarm signal in accordance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* Section 4.2.4.

8.2 Holdup Alarm Systems.

8.2.1 Installation.

8.2.1.1 The installation of holdup devices shall meet the requirements of UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems.*

8.2.1.2 Fixed-in-place holdup alarm initiating devices shall be mounted at a height that is accessible from their normal work position to the individuals responsible for utilizing the device.

8.2.2 Operation.

8.2.2.1 A holdup alarm initiating device shall lock into the alarm position or shall display a visual indication when it is operated.

8.2.2.2 Visual displays of the operation of a holdup device shall be permitted at the device, at the control unit to which it is connected, or at the location where the holdup alarm signal is received.

8.2.2.3 Visual indication of the operation of a holdup device shall require a manual operation to reset it.

8.2.2.4 Each holdup alarm initiating device shall require positive, intentional action to initiate a holdup alarm signal.

8.2.2.5 Operation of a holdup alarm initiating device shall not result in an audible signal at the protected premises or a visual signal that can be observed by an attacking party.

8.2.2.6 Each holdup alarm initiating device shall be located so that it cannot be observed by the public.

8.2.2.7 The operation of a holdup alarm initiating device shall not be obvious to an attacking party.

8.2.2.8* Each employee expected to use a holdup alarm initiating device shall be instructed in the operation of the device.

8.2.2.9* A holdup signal shall be transmitted to a constantly attended law enforcement center equipped for broadcasting instructions to response vehicles or to a constantly attended location that is approved by the AHJ.

8.3 Duress Alarm Systems.

8.3.1 Installations.

8.3.1.1 Audible and visual signaling devices shall be located at a point that is visible from the location of the duress alarm initiating device.

8.3.1.2 Fixed-in-place duress alarm initiating devices shall be installed within 1.2 m (4 ft) of the workstation and accessible from their normal work position to the individuals responsible for utilizing the device.

8.3.1.3 Portable duress alarm initiating devices shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* Section 4.2.4.

8.3.2 Operation.

8.3.2.1 A duress alarm initiating device shall lock into the alarm position or shall display a visual indication when it is operated.

8.3.2.2 Visual displays of the operation of a duress device shall be permitted at the device, at the control unit to which it is connected, or at the location where the duress alarm signal is received.

8.3.2.3 Visual indication of the operation of a duress device shall require a manual operation to reset it.

8.3.2.4 Each duress alarm initiating device shall require positive, intentional action to initiate a duress alarm signal.

8.3.2.5* Operation of a duress alarm initiating device shall result in an audible signal or a visual signal at the location of the initiating device or at a staffed location elsewhere on the protected property.

8.3.2.6 Private Duress Alarm Systems.

8.3.2.6.1 Each duress alarm initiating device shall be located so that it cannot be observed by the public.

8.3.2.6.2 The activation of a duress alarm initiating device shall not be obvious to a hostile party.

8.3.2.6.3 Each person expected to use a duress alarm initiating device shall be instructed in the operation of the device.

8.3.2.7 Public Duress Alarm Systems.

8.3.2.7.1 Each duress alarm initiating device shall be located so that it can be observed by the public.

8.3.2.7.2 Each duress alarm initiating device shall be capable of being operated by the public.

8.3.2.7.3 Instructions for the operation of each alarm initiating device shall be clearly visible to a user of the device.

8.4 Ambush Alarm Systems.

8.4.1 Installation. Ambush alarm initiating devices shall be located in or adjacent to the mechanism that is used to disarm the intrusion detection system.

8.4.2 Operation.

8.4.2.1* The initiation of an ambush signal shall be accomplished by entering a code sequence that is not similar to any code sequence that is used to perform any other operation in access control, intrusion detection, and holdup or duress systems.

8.4.2.1.1* Alarms that are manually initiated at an arming station shall require a double action trigger.

8.4.2.2 Operation of an ambush alarm initiating device shall not result in an audible signal at the protected premises or a visual signal that can be observed by an attacking party.

8.4.2.3 The operation of an ambush alarm initiating device shall not be obvious to an attacking party.

8.4.2.4* Each person expected to use an ambush alarm initiating device shall be instructed in the operation of the device.

8.4.2.5* An ambush alarm signal shall be transmitted to a constantly attended law enforcement center equipped for broadcasting instructions to response vehicles or to a constantly attended off-premises location that is approved by the AHJ.

Chapter 9 Testing and Inspections

9.1* Scope. This chapter shall cover the minimum requirements for the inspection, testing, and maintenance of electronic premises security systems as specified in Section 4.7.

9.1.1 This chapter shall apply to those systems installed under the provisions of this standard.

9.1.2 Inspection, testing, and maintenance programs shall do the following:

(1) Satisfy the requirements of this standard
(2) Conform to the equipment manufacturer's recommendations
(3) Verify correct operation of the electronic premises security systems

9.1.3* The owner or the responsible party shall be responsible for the inspection, testing, and maintenance of the system and alterations to the system.

9.1.4* When the delegation of the responsibility for 9.1.3 is transferred to a third party, it shall be given in writing with a copy of such delegation provided to the AHJ upon request and noted on the record of completion documents on premises with each addition of changes.

9.2 Impairments.

9.2.1* System defects and malfunctions shall be corrected.

9.2.1.1 The repair shall begin within 24 hours of the indication that repair is required.

9.2.2* When it is determined that there is not a risk to the protected property or the occupants, repair to the system shall be permitted to begin outside of the time period required by 9.2.1.1 if the owner or responsible party is notified in writing.

9.2.3 If a defect or malfunction is not corrected at the conclusion of system inspection, testing, or maintenance, written notice shall be provided to the system owner or responsible party within 24 hours.

9.2.4 A record shall be maintained by the system owner or responsible party for a period of 1 year from the date the impairment is corrected.

9.3 General Testing, Inspection, and Maintenance.

9.3.1 Nothing in Chapter 9 shall be intended to prevent the use of alternate test methods or testing devices.

9.3.2 Alternate test methods or testing devices shall provide the same level of effectiveness and safety.

9.3.3 Alternate test methods shall meet the intent of the requirements of Chapter 9.

9.3.4 Inspection, testing, or maintenance shall be permitted to be performed by a person or organization other than the owner if conducted under a written contract.

9.3.5 Service Personnel.

9.3.5.1 Service personnel shall be qualified and experienced in the inspection, testing, and maintenance of electronic premises security systems.

9.3.5.2 Examples of qualified personnel shall be permitted to include but shall not be limited to individuals with the following qualifications:

(1)*Factory trained and certified
(2) Certified or licensed by state or local authority
(3) Trained and qualified personnel employed by an organization listed by a national testing laboratory for the servicing of electronic premises security systems

9.3.6 Notification.

9.3.6.1* Before proceeding with any testing or maintenance, all persons and facilities receiving alarm, supervisory, or trouble signals and all building occupants shall be notified of the testing or maintenance to prevent unnecessary response.

9.3.6.2 At the conclusion of the testing, those previously notified shall be notified that the testing has been concluded.

9.3.6.3 The owner or the responsible party and service personnel shall coordinate system testing to prevent interruption of critical facility systems or equipment.

9.3.7 Prior to system maintenance or testing, the information regarding the system and system alterations, including record of completion, owner's manual, and installation instructions, shall be provided by the owner or responsible party to the service personnel upon request.

9.4 System Testing.

9.4.1 Acceptance Testing. All new systems shall be inspected and tested in accordance with the requirements of 9.4.3.

9.4.2 Reacceptance Testing.

9.4.2.1 Reacceptance testing shall be performed after any of the following:

(1) Added or deleted system components
(2) Any modification, repair, or adjustment to system hardware or wiring
(3) Any change to site-specific software
(4) Any modifications to the structure being protected

9.4.2.2 All components, circuits, systems operations, or site-specific software functions known to be affected by the change or identified by a means that indicates the changes shall be tested.

9.4.2.3 A revised record of completion in accordance with 4.7.2.1 shall be prepared to reflect any changes to the original and subsequent inspections attached as addenda to this current document.

9.4.3 Test Methods. Electronic premises security systems and other systems and equipment that are associated with security systems and accessory equipment shall be tested according to Table 9.4.3(a) and Table 9.4.3(b).

Table 9.4.3(a) Test Methods

Device	Method
Control Equipment	
(1) Function	At a minimum, control equipment shall be tested to verify correct receipt of alarm, supervisory, and trouble signals; auxiliary functions (outputs); circuit supervision, including detection of open circuits and ground faults; and power supply supervision for detection of loss of ac power and disconnection of secondary batteries.
(2) Fuses	The rating and supervision shall be verified.
(3) Interfaced equipment	Integrity of single or multiple circuits providing interface between two or more control panels shall be verified. Interfaced equipment connections shall be tested by operating or simulating operation of the equipment being supervised. Signals required to be transmitted shall be verified at the control panel.
(4) Lamps and LEDs	Lamps and LEDs shall be illuminated.
(5) Primary (main) power supply	All secondary (standby) power shall be disconnected and tested under maximum load, including all alarm appliances requiring simultaneous operation. All secondary (standby) power shall be reconnected at end of test. For redundant power supplies, each shall be tested separately.
Engine-Driven Generator	If an engine-driven generator dedicated to the electronic premises security system is used as a required power source, operation of the generator shall be verified in accordance with NFPA 110, *Standard for Emergency and Standby Power Systems,* by the building owner.
Secondary (Standby) Power Supply	All primary (main) power supplies shall be disconnected and the occurrence of required trouble indication for loss of primary power shall be verified. The system's standby and alarm current demand shall be measured or verified and, using manufacturer's data, the ability of batteries to meet standby and alarm requirements shall be verified. Sounders shall be operated for a minimum of 5 minutes. Primary (main) power supply shall be reconnected at end of test.
Uninterrupted Power Supply (UPS)	If a UPS system dedicated to the electronic premises security system is used as a main power source, operation of the UPS system shall be verified by the building owner in accordance with NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*.
Batteries — General Tests	Prior to conducting any battery testing, the person conducting the test shall ensure that all system software stored in volatile memory is protected from loss.
(1) Visual inspection	Batteries shall be inspected for corrosion or leakage. Tightness of connections shall be checked and ensured. If necessary, battery terminals or connections shall be cleaned and coated. Electrolyte level in lead-acid batteries shall be visually inspected.
(2) Battery replacement	Batteries shall be replaced in accordance with the recommendations of the electronic premises security system manufacturer or when the recharged battery voltage or current falls below the manufacturer's recommendations.
(3) Charger test	Operation of battery charger shall be checked in accordance with charger test for the specific type of battery.
(4) Discharge test	With the battery charger disconnected, the batteries shall be load tested following the manufacturer's recommendations. The voltage level shall not fall below the levels specified. An artificial load equal to the full electronic premises security system shall be permitted to be used in conducting this test.
(5) Load voltage test	With the battery charger disconnected, the terminal voltage shall be measured while supplying the maximum load required by its application. The voltage level shall not fall below the levels specified for the specific type of battery. If the voltage falls below the level specified, the corrective action shall be taken and the batteries shall be retested. An artificial load equal to the full electronic premises security system shall be permitted to be used in conducting this test.

Table 9.4.3(a) ***Continued***

Device	Method
Battery Tests (Specified Types)	
(1) Primary battery load voltage test	The maximum load for a No. 6 primary battery shall not be more than 2 amperes per cell. An individual (1.5 volt) cell shall be replaced when a load of 1 ohm reduces the voltage below 1 volt. A 6 volt assembly shall be replaced when a load of 4 ohms reduces the voltage below 4 volts.
(2) Lead-acid type	Charger test: With the batteries fully charged and connected to the charger, the voltage across the batteries shall be measured with a voltmeter. The voltage shall be 2.30 volts per cell ±0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. Load voltage test: Under load, the battery shall not fall below 2.05 volts per cell. Specific gravity test: The specific gravity of the liquid in the pilot cell or all cells shall be measured as required. The specific gravity shall be within the range specified by the manufacturer. Although the specific gravity varies from manufacturer to manufacturer, a range of 1.205 to 1.220 volts is typical for regular lead-acid batteries, while 1.240 to 1.260 volts is typical for high-performance batteries. A hydrometer that shows only a pass or fail condition of the battery and does not indicate the specific gravity shall not be used, because such a reading does not give a true indication of the battery condition.
(3) Nickel-cadmium type	Charger test: With the batteries fully charged and connected to the charger, an ampere meter shall be placed in a series with the battery under charge. The charging current shall be in accordance with the manufacturer's recommendations for the type of battery used. In the absence of specific information, 1/30 to 1/25 of the battery rating shall be used. Load voltage test: Under load, the float voltage for the entire battery shall be 1.42 volts per cell, nominal. If possible, cells shall be measured individually.
(4) Sealed lead-acid type	Charger test: With the batteries fully charged and connected to the charger, the voltage across the batteries shall be measured with a voltmeter. The voltage shall be 2.30 volts per cell ±0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. Load voltage test: Under load, the battery shall perform in accordance with the battery manufacturer's specifications.
Transient Suppressors	Lightning protection equipment shall be inspected and maintained per the manufacturer's specifications. Additional inspections shall be required after any lightning strikes. Equipment located in moderate to severe areas outlined in NFPA 780, *Standard for the Installation of Lightning Protection Systems,* Appendix H, shall be inspected semi-annually and after any lightning strikes.
Sounding and Visual Devices	
(1) Audible	Sound pressure levels shall be measured with sound level meter meeting ANSI S1.4, *Specification for Sound Level Meters,* Type 2 requirements. Levels throughout the area covered by the sounder shall be measured and recorded.
(2) Visible	Tests shall be performed in accordance with the manufacturer's instructions.
Transmitting Equipment	Reserved
Interface Equipment	Interface equipment connections shall be tested by operating or simulating the equipment being supervised. Signals required to be transmitted shall be at the control panel. Test frequency for interface equipment shall be the same as the frequency required by the applicable NFPA standard(s) for the equipment being supervised.

(continues)

Table 9.4.3(a) ***Continued***

Device	Method
Low-Powered Radio (Wireless Systems)	The following procedures describe additional acceptance and reacceptance test methods to verify wireless protection system operation: The manufacturer's manual provided by the system supplier shall be used to verify correct operation after the initial testing phase has been performed by the supplier or by the supplier's designated representative. Starting from the functional operating condition, the system shall be initialized in accordance with the manufacturer's manual. A test shall be conducted to verify the alternative path, or paths, by turning off or disconnecting the primary wireless repeater. The alternative communications path shall exist between the wireless control panel and the peripheral devices used to establish initiation, indication, control, and annunciation. The system shall be tested for both alarm and trouble conditions. Batteries for all components in the system shall be checked monthly. If the control panel checks all batteries and all components daily, the system shall not require the monthly testing of the batteries.
Annunciators	The correct operation and identification of annunciators shall be verified. If provided, the correct operation of annunciators under a fault condition shall be verified.
Conductors — Metallic	
(1) Stray voltage	All installation conductors shall be tested with a volt/ohmmeter to verify that there are no stray (unwanted) voltages between installation conductors or between installation conductors and ground. Unless a different threshold is specified in the system per the installed equipment manufacturer's specifications, the maximum allowable stray voltages shall not exceed 1 volt ac/dc.
(2) Ground faults	All installation conductors other than those intentionally and permanently grounded shall be tested for isolation from ground per the installed equipment manufacturer's specifications.
(3) Short-circuit faults	All installation conductors other than those intentionally connected together shall be tested for conductor-to-conductor isolation per the installed equipment manufacturer's specifications. The same circuits also shall be tested conductor-to-ground.
(4) Loop resistance	With each initiating and indicating circuit installation conductor pair short-circuited at the far end, the resistance of each circuit shall be measured and recorded. It shall be verified that the loop resistance does not exceed the installed equipment manufacturer's specified limits.
(5) Supervision	Introduction of a fault in any circuit monitored for integrity shall result in a trouble indication at the control unit. One connection shall be opened for not less than 10 percent of the initiating devices, sounders, and controlled devices on every initiating device circuit and sounder circuit.
Conductors — Nonmetallic	
(1) Circuit integrity	Each initiating device and sounder circuit shall be tested to confirm that the installation conductors are monitored for integrity.
(2) Fiber optics	The fiber-optic transmission line shall be tested in accordance with the manufacturer's instructions by the use of an optical power meter or by an optical time domain reflectometer used to measure the relative power loss of the line. This relative figure for each fiber-optic line shall be recorded in the electronic premises security system control panel. If the power level drops 2 percent or more from the value recorded during the initial acceptance test, the transmission line, section thereof, or connectors shall be repaired or replaced by a qualified technician to bring the line back into compliance with the accepted transmission level per the manufacturer's recommendations.
(3) Supervision	Introduction of a fault in any supervised circuit shall result in a trouble indication at the control unit. One connection shall be opened at not less than 10 percent of the initiating device and sounders. Each initiating device and sounder circuit shall be tested for correct indication at the control unit.

Table 9.4.3(b) Test Methods of Initiating Devices

Intrusion Detection Device	Method
Audio Sensors	Using a sound level meter designed, constructed, and calibrated in accordance with ANSI S1.4, *Specification for Sound Level Meters*, determine the average ambient sound does not exceed 65 dBA during the period the intrusion detection system is armed. The area covered by a single detector shall not exceed the area of coverage specified by the detector manufacturer. Utilizing the method recommended by the manufacturer, test the operation of the system.
Contacts (1) Door (2) Window	 Open the door. Open the window.
Exterior Buried Detectors	Reserved
Glass Break Detectors (1) Audio (2) Shock	 Using a noise generation device recommended by the manufacturer to simulate the sound of breaking glass and create a noise at the surface of the glass. Using a test device recommended by the manufacturer, simulate the breaking of glass.
Motion Detection (1) PIR (2) Microwave (3) Dual Tech	 Walk across the furthest point of the field of detection from the detector in an upright position at a rate of one 760 mm ± 80 mm (30 in. ± 3 in.) per second. Walk into the furthest point of the field of detection from the detector in an upright position at a rate of one 760 mm ± 80 mm (30 in. ± 3 in.) per second. Walk diagonally across the furthest point of the field of detection from the detector in an upright position at a rate of one 760 mm ± 80 mm (30 in. ±3 in.) per second.
Photo Electric Detection	Disrupt the channel of detection by passing an object through the channel.
Pressure and Stress Sensors	Reserved
Protective Cable	Reserved
Proximity Sensors	Reserved
Shock Sensors	Reserved
Sound Detection — Vault	Using a sound level meter designed, constructed, and calibrated in accordance with ANSI S1.4, *Specification for Sound Level Meters*, determine the system is adjusted to transmit an alarm at sound levels of 80 to 90 dBA for a sound of impact origin in reverberant vaults. In nonreverberant vaults, systems shall be adjusted to transmit an alarm at a sound level 15 dBA above the intended ambient for the vault for impact-generated sounds.
Holdup Devices (1) Fixed in Place (2) Portable	 Simulate a holdup alarm condition by activating the device. Simulate a holdup alarm condition by activating the device at the maximum distance of the area of intended use.

(continues)

Table 9.4.3(b) ***Continued***

Intrusion Detection Device	Method
Duress Devices	
(1) Fixed in Place	Simulate a duress condition by activating the device.
(2) Portable	Simulate a duress condition by activating the device at the maximum distance of the area of intended use.
Ambient Devices	
(1) Fixed in Place	Simulate an ambush alarm condition by activating the device.
(2) Portable	Simulate an ambush condition by activating the device at the maximum distance of the area of intended use.
Access Control Components	**Method**
Controller	Reserved
Reader	
(1) Key	Reserved
(2) Magnetic Stripe	Reserved
(3) RFID Card	Reserved
(4) Biometric	Reserved
Position Sensor	Reserved
Electric Latch	Reserved
Electric Lock	Reserved
Electromagnetic — Lock	Reserved
Request to Exit	
(1) Manual	Reserved
(2) Motion	Reserved
CCTV Devices	**Method**
Video Controller	Reserved
Video Switcher	Reserved
Monitor	Reserved
Camera	Reserved
Enclosure	Reserved

9.5 Inspection and Testing Frequency. Electronic premises security systems and other systems and equipment that are associated with security systems and accessory equipment shall be tested at the frequencies according to Table 9.5.

Table 9.5 Test Frequency

Device	Frequency
Intrusion detection system	Annually
(1) Exterior detectors	Semiannually
(2) Interior detectors	Annually
Holdup, Duress, or Ambush System	Annually
(1) Portable devices	Semiannually
(2) Exterior fixed devices	Quarterly
(3) Interior fixed devices	Annually
Access control system	Annually
(1) Readers	Annually
(2) Position switches	Quarterly
(3) Electric hardware	Quarterly
(4) Request-to-exit devices	Annually
CCTV system	Annually
(1) Camera enclosures	Annually before adverse weather conditions
(2) Recorders	Quarterly
Sounding devices	Quarterly
Batteries — general tests	Annually
Off-premises transmission equipment	Quarterly or by automatic daily test
Interface equipment	Annually

Annex A Explanatory Material

Annex A is not a part of the requirements of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.3.1 Words used in the present tense include the past tense; words used in the masculine gender include the feminine and neuter; the singular number includes the plural, and the plural number includes the singular.

A.3.2.1 Approved. The National Fire Protection Association does not approve, inspect, or certify any installations, procedures, equipment, or materials; nor does it approve or evaluate testing laboratories. In determining the acceptability of installations, procedures, equipment, or materials, the authority having jurisdiction may base acceptance on compliance with NFPA or other appropriate standards. In the absence of such standards, said authority may require evidence of proper installation, procedure, or use. The authority having jurisdiction may also refer to the listings or labeling practices of an organization that is concerned with product evaluations and is thus in a position to determine compliance with appropriate standards for the current production of listed items.

A.3.2.2 Authority Having Jurisdiction (AHJ). The phrase "authority having jurisdiction," or its acronym AHJ, is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his or her designated agent assumes the role of the authority having jurisdiction; at government installations, the commanding officer or departmental official may be the authority having jurisdiction.

A.3.2.4 Listed. The means for identifying listed equipment may vary for each organization concerned with product evaluation; some organizations do not recognize equipment as listed unless it is also labeled. The authority having jurisdiction should utilize the system employed by the listing organization to identify a listed product.

A.3.3.1 Access Control. Access control portals are doors, gates, turnstiles, and so forth. Controls can be operational, technical, or physical or a combination thereof and can vary depending on type of credential, authorization level, day, or time of day.

A.3.3.2 Active Lock. Examples of active locks are electromagnets, electric locks that do not allow egress, and other locking devices that control egress as well as ingress.

A.3.3.3 Ancillary Functions. Examples of ancillary functions are environmental monitor points, fire detection points, turning lights on and off, control of heating and air conditioning equipment, or tracking attendance.

A.3.3.4 Annunciator. An annunciator can log alarms or display a continuous status of devices or systems. The annunciator can signal audibly, visually, or both to indicate a change of status.

A.3.3.5 Closed Circuit Television (CCTV). The closed circuit signal can connect by, but is not limited to, coaxial, CAT.5, fiber optics, microwave, radio frequency (RF), or infrared.

A.3.3.9.1.2 Duress Alarm Initiating Device. A hostile situation can be an intruder. Often these alarms are triggered by unobtrusive sensors so as not to place the victim in greater danger. Duress alarms can be designed to silently initiate an alarm, which is annunciated at a remote station or guard post.

A.3.3.9.1.3 Holdup Alarm Initiating Device. A holdup device at the protected premises can be at a bank teller window or store cash register. It is usually a silent alarm to protect the cashier.

A.3.3.11 False Alarm. A false alarm can result from a fault or problem in the system, from an environmental condition, or operation by the user of the system causing an unwanted condition.

A.3.3.12 Foil. Foil is a thin metallic strip between 0.0254 mm (0.001 in.) and 0.00762 mm (0.0003 in.) in thickness, and from 3.175 mm (0.125 in.) to 25.4 mm (1.0 in.) in width. Foil, also known as tape, is commonly used on windows and other glass installations. When the glass is broken, the foil breaks and opens the electrical circuit, causing an alarm condition.

A.3.3.14 Monitoring Station. Services offered by a monitoring station can include the following:

(1) System installation
(2) Alarm, guard, and supervisory signal monitoring

(3) Retransmission
(4) Testing and maintenance
(5) Alarm response service
(6) Record keeping and reporting

A.3.3.17 Reader. Readers can be of many types and are intended to include car tags, electronic key, magnetic stripe, proximity badge, biometric, or other identifier.

A.3.3.20 Screens. Skylights and crawl spaces can be protected by screens. The screen can detect intrusion by use of a broken circuit or by capacitance techniques.

A.3.3.22.1 Alarm Signals. Alarm signals come from many different systems such as intrusion detection, ambush, duress, holdup alarms, and access control. These systems are defined in this standard for purposes of equipment installation. However, telling dispatching agencies the type of system is not always necessarily of help to the police or guard responding to these alarms. In the simplest terms, dispatching agencies need the following information:

(1) Address
(2) Name of business at protected premises
(3) Type of alarm (automatic or manual)
(4) Class (audible or silent)
(5) Premises (commercial, factory, bank, mercantile, jewelry store, etc.)
(6) Location at premises (zone or area of building)
(7) Device type (motion detector, glass break, door contact, etc.)
(8) Verification attempted (yes or no)
(9) Verification type (call, video, third party)

A.3.3.24.2 Digital Imaging System (DIS). Digital video can connect by, but is not limited to, coaxial, CAT.5, fiber optics, microwave, infrared, local area network (LAN), or wide area network (WAN).

A.3.3.24.6 Integrated System. Other systems include, but are not limited to, fire alarm, building automation, lighting, and administrative controls.

A.3.3.25.1 Ball Trap. Such devices are intended to secure a conductor that is used to protect an air conditioner or similar opening so that the circuit is interrupted if the conductor is removed or cut.

A.3.3.25.3 Disconnecting Trap. Such devices are designed to allow the disassembly of the device without the use of tools for the purpose of servicing such objects. These devices are installed in such a manner that a protective circuit is interrupted if the conductor or cord is cut or moved.

A.3.3.26 Vault. A vault can also consist of a door and modular panels constructed in compliance with the requirements in UL 608, *Standard for Burglary-Resistant Vault Doors and Modular Panels*.

A.4.1.6 Examples of qualified personnel include individuals who can demonstrate experience on similar systems that they are designing. The designer has to take into consideration the threat that the system is being designed for as well as provisions to minimize the possibility of false alarms.

A.4.1.7 The installers of electronic premises security systems should be familiar with the equipment that they are to install. This includes knowing the 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 AHJ for the type of system being installed.

A.4.2.3.3 The designer for other electronic premises security systems can include secondary power requirements depending on the risk assessment and design objectives of the systems.

A.4.2.6.1 Secondary power for electronic premises security systems can be based on the risk assessment and design. Consideration should be given to whether access to the system is readily available and 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.

A.4.5.2 Examples of environmental factors that should be considered include, but are not limited to, the following:

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

A.4.5.6.3 Additional information on this subject can be found in NFPA 70, *National Electrical Code*, Article 110.

A.4.5.8.2 A splice intended to be soldered should be joined mechanically before being soldered. Each splice and joint should be covered 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 device manufacturer's supplied leads should be either:

(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 of the strands of the conductor that are bent and/or misshapen and/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 provide adequate strain relief so that a firm tug does not break or damage the connection.

A.4.5.8.3 The intent of this requirement is to shield the wiring from induction of ac. In accordance with NFPA 70, *National Electrical Code*, all metallic raceway is bonded to ground.

A.4.5.8.6 Some examples of properly mounted devices and protected the 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 metal raceway should not be more than 7.62 cm (3 in.) apart.
(2) The orientation of the installed metal raceway relative to the installed device should be so as to facilitate the 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 5.08 cm (2 in.). The wires or cables should be cut so that, including its stripped end, the wires or cables extend at least 15.24 cm (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, the manufacturer 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 they should be connected. The stripped portion of the conductor should have the same number of conductors as the unstripped portion.

A.4.5.9 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.

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

A.4.5.9.3.1 This requirement is not intended to preclude verification and local test intervals prior to alarm transmission.

A.4.5.9.4.1 Examples of interference are impulse noise and adjacent channel interference.

A.4.5.11.1 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.

A.4.5.11.2.1 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.

A.4.5.11.2.3 If the system serves more than one building, each building should be indicated separately.

A.4.5.13.3 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:
    (a) Reconfigure the site-specific data held within or controlled by the electronic premises security system
    (b) 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.

A.4.7.2.1 Examples of owners or responsible parties include, but are not limited to, the owner of the protected property, the lease holder of the tenant space where the system is installed, an employee or agent of the owner or the lease holder, or the like.

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.

A.4.7.2.1(1) 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 and as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed. This information should include the following:
    (a) Listing of the individual system components that require periodic testing and maintenance.
    (b) Step-by-step instructions detailing the requisite testing and maintenance procedures, and the intervals at which these procedures should be performed, for each type of device installed.
    (c) A schedule that correlates the testing and maintenance procedures recommended in Chapter 9.
    (d) Detailed troubleshooting instructions for each trouble condition generated from monitored field wiring, including opens, grounds, and loop failures. [These instructions should include a list of all trouble signals annunciated by the system, a description of the conditions(s) that cause such trouble signals, and step-by-step instructions describing how to isolate such problems and correct them (or how to 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) Typical examples of Record of Completion forms are shown in Figure A.4.7.2.1(3)(a) through Figure A.4.7.2.1(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 ❑ Video surveillance

❑ 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:

Mfg.: _____ Mfg.: _____ Mfg.: _____

Model: _____ Model: _____ Model: _____

Transmission type: _____ Transmission type: _____ 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: _____

© 2005 National Fire Protection Association NFPA 731 (p. 1 of 1)

FIGURE A.4.7.2.1(3)(a) Record of Completion Report.

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS INSPECTION & TESTING REPORT

SYSTEM DESCRIPTION

Type of System:
(Check only one; use additional forms for other systems at same premises)

- ❑ Exterior intrusion detection
- ❑ Interior intrusion detection
- ❑ Holdup system
- ❑ Duress system
- ❑ Ambush system

Control Unit:

Mfg.: _____

Model: _____

Type of Circuit:

- ❑ End of line Number of circuits: _____
- ❑ Addressable Number of addresses: _____
- ❑ Wireless Number of transmitters: _____

DETECTION DEVICES

Quantity	Type of Detection	Device Type or Model
_____	Audio sensors	_____
_____	Contacts — door	_____
_____	Contacts — window	_____
_____	Exterior buried detectors	_____
_____	Motion detection	_____
_____	Photo electric detection	_____
_____	Pressure & stress sensors	_____
_____	Protective cable	_____
_____	Protective wiring	_____
_____	Proximity sensors	_____
_____	Shock sensors	_____
_____	Sound detection	_____
_____	Holdup devices — portable	_____
_____	Holdup devices — fixed in place	_____
_____	Duress devices — portable	_____
_____	Duress devices — fixed in place	_____
_____	Ambush devices	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____

SIGNALING DEVICES

Location	Quantity	Type
❑ None		
❑ Interior	_____	❑ Bell ❑ Siren ❑ Horn ❑ Other _____
❑ Exterior	_____	❑ Bell ❑ Siren ❑ Horn ❑ Other _____

NOTIFICATION OF TESTING

Notify premise's owner or responsible party:

Name: _____ Date _____ Time _____

Monitoring station:

Name: _____ Date _____ Time _____

© 2005 National Fire Protection Association

FIGURE A.4.7.2.1(3)(b) Intrusion Detection or Holdup and Duress Systems Report.

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS INSPECTION & TESTING REPORT (continued)

SYSTEM INSPECTION AND TEST

Component	**Visual Check**		**Functional Test**		**Comments**
	Yes	No	Pass	Fail	
Control unit	☐	☐	☐	☐	
Arming means	☐	☐	☐	☐	
Primary power circuit disconnect	☐	☐	☐	☐	
Secondary power	☐	☐	☐	☐	
Batteries	☐	☐	☐	☐	
Voltage at end of test	☐	☐	☐	☐	
Generator records	☐	☐			
Signaling device(s)	☐	☐	☐	☐	
Protective circuit supervision	☐	☐	☐	☐	

DETECTION DEVICE INSPECTION AND TEST

Location/Address	**Visual Check**		**Functional Test**		**Results/Explanation**
	Yes	No	Pass	Fail	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

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

© 2005 National Fire Protection Association

NFPA 731 (p. 2 of 3)

FIGURE A.4.7.2.1(3)(b) *Continued*

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS INSPECTION & TESTING REPORT (continued)

TRANSMISSION TEST

Signal/Component	Yes	No	Time	Comments
Line security	❑	❑		
Alarm signal	❑	❑		
Supervisory signal	❑	❑		
Trouble signal	❑	❑		
Other:	❑	❑		

FINAL TEST REPORT

The following did not operate properly: _____

NOTIFICATION OF END OF TESTING

Notify premises owner or responsible party:

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: _____

Owner or responsible party: _____ Date: _____

Signature: _____ Time: _____

© 2005 National Fire Protection Association NFPA 731 (p. 3 of 3)

FIGURE A.4.7.2.1(3)(b) ***Continued***

ACCESS CONTROL INSPECTION & TESTING REPORT

COMPONENTS

Quantity	Type of Components	Device Type or Model
_____	Controller	_____
_____	Power supply	_____
_____	Reader	_____
_____	Key	_____
_____	Magnetic stripe	_____
_____	RFID card	_____
_____	Biometric	_____
_____	Position sensor	_____
_____	Electric latch	_____
_____	Electric lock	_____
_____	Electromagnetic lock	_____
_____	Request to exit	_____
_____	Manual	_____
_____	Motion	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

NOTIFICATION OF TESTING

Notify premise's owner or responsible party:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

SYSTEM INSPECTION AND TEST

Component	Visual Check		Functional Test		Comments
	Yes	No	Pass	Fail	
Control unit	❑	❑	❑	❑	_____
Primary power circuit disconnect	❑	❑	❑	❑	_____
Secondary power	❑	❑	❑	❑	_____
Batteries	❑	❑	❑	❑	_____
Voltage at end of test	❑	❑	❑	❑	_____
Generator records	❑	❑			_____
Power supply	❑	❑	❑	❑	_____

© 2005 National Fire Protection Association NFPA 731 (p. 1 of 3)

FIGURE A.4.7.2.1(3)(c) Access Control Report.

ACCESS CONTROL
INSPECTION & TESTING REPORT (continued)

COMPONENT INSPECTION AND TEST

Location/Address	Visual Check		Functional Test		Results/Explanation
	Yes	No	Pass	Fail	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	

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

© 2005 National Fire Protection Association NFPA 731 (p. 2 of 3)

FIGURE A.4.7.2.1(3)(c) ***Continued***

ACCESS CONTROL
INSPECTION & TESTING REPORT (continued)

TRANSMISSION TEST

Signal	Yes	No	Time	Comments
Alarm signal	❑	❑	_____	_____
Trouble signal	❑	❑	_____	_____

FINAL TEST REPORT

The following did not operate properly: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

NOTIFICATION OF END OF TESTING

Notify premise's owner or responsible party:

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: _____

Owner or responsible party: _____ Date: _____

Signature: _____ Time: _____

© 2005 National Fire Protection Association NFPA 731 (p. 3 of 3)

FIGURE A.4.7.2.1(3)(c) ***Continued***

VIDEO SURVEILLANCE INSPECTION & TESTING REPORT

COMPONENTS

Quantity	Type of Components	Device Type or Model
_____	Video controller	_____
_____	Video switcher	_____
_____	Video multiplexer	_____
_____	Monitor (monochrome or color)	_____
_____	Recorder (Tape or DVR)	_____
_____	Camera	_____
_____	Enclosure	_____
_____	Pan tilt zoom (PTZ)	_____
_____	Alarming inputs	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

NOTIFICATION OF TESTING

Notify premise's owner or responsible party:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

SYSTEM INSPECTION AND TEST

Component	Visual Check		Functional Test		Comments
	Yes	No	Pass	Fail	
Control unit	❑	❑	❑	❑	_____
Primary power circuit disconnect	❑	❑	❑	❑	_____
Secondary power	❑	❑	❑	❑	_____
Batteries	❑	❑	❑	❑	_____
Voltage at end of test	❑	❑	❑	❑	_____
Generator test records	❑	❑			_____
Remote controls	❑	❑	❑	❑	_____
Variable lenses	❑	❑	❑	❑	_____

© 2005 National Fire Protection Association NFPA 731 (p. 1 of 2)

FIGURE A.4.7.2.1(3)(d) Video Surveillance Test Report.

VIDEO SURVEILLANCE INSPECTION & TESTING REPORT (continued)

COMPONENT INSPECTION AND TEST

Location/Address	Visual Check		Functional Test		Results/Explanation
	Yes	No	Pass	Fail	
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____

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

TRANSMISSION TEST

Signal	Yes	No	Time	Comments
Digital signal	❑	❑	_____	_____

FINAL TEST REPORT

The following did not operate properly: _____

_____

_____

_____

_____

_____

NOTIFICATION OF END OF TESTING

Notify premise's owner or responsible party:

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: _____

Owner or responsible party: _____ Date: _____

Signature: _____ Time: _____

© 2005 National Fire Protection Association NFPA 731 (p. 2 of 2)

FIGURE A.4.7.2.1(3)(d) ***Continued***

ADDITIONAL DEVICES
INSPECTION & TESTING REPORT

COMPONENT INSPECTION AND TEST

Type/Location/Address	Visual Check Yes	Visual Check No	Functional Test Pass	Functional Test Fail	Results/Explanation
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	

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

Additional devices System type: ______________________

© 2005 National Fire Protection Association NFPA 731 (p. 1 of 1)

FIGURE A.4.7.2.1(3)(e) Additional Devices Test Report.

A.4.7.2.2.1 This training should be based upon the level of involvement with the system that the user can have. This level can be as simple as how to arm and disarm an intrusion detection system to as complex as setting 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.4.7.2.2.2 This 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.5.2.4.1.2(1) A single stacked PEC unit with two or more beams can be used as a substitute, provided that two beams are broken before signal initiation.

A.5.4.1.3(4) To provide detection of "burning bars," heat and smoke detectors can be used so as to detect the products of combustion and heat. When used in this application, the requirements of *NFPA 72, National Fire Alarm Code*, are not intended to be met.

A.5.4.1.3(6) See A.5.4.1.3(4).

A.6.1.2 Examples of portals include, but are not limited to, doors, gates (personnel and vehicular), lift gates, sliders, barriers, turnstiles (mechanical and optical), man-traps, and sally-ports.

A.6.1.3 Readers include, but are not limited to, magnetic stripe, radio frequency identification (RFID) (long and short range), bar code, keypad, Wiegand, biometrics, and smart cards (contact and contactless), or any device that provides a unique identity of the card or person. Based on the threat level, systems can employ a single reader or a combination of these devices.

A.6.1.3.1 The requirements of the Americans with Disabilities Act and other applicable standards should be considered when selecting mounting criteria.

A.6.1.3.3 Examples of use would be in health care facilities where gurneys or other such appliances can be in use.

A.6.1.3.7 The actual interval of time should be as short as possible. Typically, most systems complete this sequence within 3 seconds or less. The 10-second interval that is cited within the main body of this standard is the maximum time allowed.

A.6.1.4.1 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 Code*, and amendments adopted by the AHJ. Based on the security vulnerability assessment of the protected premises, the designer can also consider UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

A.6.1.4.2 The installation of locking hardware should not compromise the fire rating of a door or door frame. NFPA 80, *Standard for Fire Doors and Fire Windows*, should be consulted. The manufacturer's specification for the fire-rated door and frame should also be consulted before any field modifications are made.

Locking hardware should be appropriate for the application, and repeated use should not result in the inability of the portal to be secured. Consideration should also be given to other portal hardware that can affect the ability of the portal to be secured.

Use of magnetic door locks (mag locks) on certain portals poses significant security concerns. For the purpose of life safety, many codes and standards require power interruption to magnetic door locks during fire alarm conditions or loss of primary power. Whenever magnetic lock power is interrupted, the portal can become a free point of both egress and ingress. This is not necessarily an acceptable condition for many premises. Electric portal hardware, which allows mechanical egress, can be a more secure alternative.

A.6.1.4.3 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.6.1.4.4 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 Code*, and amendments adopted by the AHJ. Based on the security vulnerability assessment of the protected premises, the designer might also wish to consider UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

A.6.1.4.5.1 A manual means of release is not necessarily required for occupancies such as penal institutions, mental hospitals, or other occupancies where direct supervision by trained staff is provided and the AHJ approves such an installation.

A.6.1.5.1 Examples of position sensors include, but are not limited to, edge sensors, gate arm limit switches, and contact switches.

A.6.1.5.2 Position sensors can also be used for other applications such as relocking, arming and disarming of an intrusion detection system, and other approved control functions. The integration of the access control system should not compromise the primary objectives of the access control system.

The use of an access control system in integration with an intrusion detection system should not create false alarms from the system not being properly disarmed prior to entry.

A.6.1.6 The two methods of authorized egress are free and controlled.

A.6.1.6.1.2 The RTE can bypass the door position switch and not be used to control the lock at the portal. If the RTE also controls the portal lock, concerns for life safety would dictate the lock fail-safe on loss of power.

A.6.1.6.2 Controlled egress can be used for applications such as anti pass-back, mustering, patient wandering, infant abduction, and two-person rule.

A.6.1.6.2.2 Controlled egress can be enforced by sounding an alarm if the portal is opened without presenting a valid credential or by preventing the opening of the portal. If opening the portal is prevented and the portal is a required means of egress, then the requirements for active locks should be used.

A.6.1.8.2 Depending upon the design of the system, one or several power supplies can be used. The power supplies should be sized to provide adequate power for simultaneous use of all associated devices, such as readers, RTE motion detectors, locks, controllers, and so forth. Power calculations need not take into account simultaneous inrush current.

As a result of certain conditions, such as temperature, device inrush requirements, tolerances, and other environmental factors, it is recommended that power supplies be designed with a safety factor of 25 percent.

A.6.2.1 The system operating parameters can be based on a security vulnerability assessment of the protected premises.

A.6.3 This standard currently applies to the protected premises. Network configurations that send data off-premises can need additional protection in the form of encryption. Current encryption schemes can be certified by National Institute of Standards and Technology (NIST) in accordance with Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. Typically, encryption schemes used for security applications employ a 128 bit algorithm.

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 it is not readily accessible to a vandal without compromising the requirements of 7.1.1.

A.7.2.5(1) The use of a heater within an enclosure might be required to protect the camera, lens, and auto iris.

A.7.2.5(2) Sunshields or sun hoods can be required to reduce glare when the sun is low on the horizon, or if the camera has a direct view of the sun or any other point light source. Whenever possible, the camera should not look directly into the sun or point light source.

A.7.2.5(3) The selection of enclosures is to be appropriate for the prevalent environmental conditions. Heaters, blowers, defrosters/defoggers, and wipers can be required.

A.7.2.5(4) Mounts and remote positioning devices should be designed to withstand local wind conditions and provide a usable image based upon the requirements of the AHJ.

A.7.2.5(5) A method should be provided so that external moisture does not impair the ability of the camera to produce a usable image as required by the AHJ.

A.7.2.6.1 If a camera has a view that looks directly into a bright light source or extremely high contrast scene, the quality of the foreground image is degraded. The camera should be relocated so that its field of view is perpendicular to the light source. The camera should be positioned so that the source of light is behind the camera.

A.7.2.6.2 The camera feature known as backlight compensation (BLC) allows the camera to be able to reduce the level of the video at the bright areas and then reproduces the overall video signal at an average video level. Most cameras now have this feature and the more advanced cameras have the means to set the parameters for each application. The installing technician should be aware of the location of the sensing windows for BLC to work correctly.

A.7.3 Low-light level conditions can be compensated in many ways. Some of these include, but are not limited to, the following:

(1) Cameras listed by their manufacturer to operate at 10 lux or less
(2) Use of light amplification devices such as a "starlight scope"
(3) Nonvisible scene illumination such as infra-red (IR) or ultra-violet (UV)

A.7.4 The choice of an enclosure should be based on application, environmental concerns, 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, 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.

A.7.5 Mounting assemblies have a few basic requirements. The selection criteria consist of the following:

(1) Overall length of the camera housing
(2) Total weight of the camera/lens/housing
(3) Type of mounting required (wall, pole, or ceiling)

When mounting equipment, the installer should consider such factors as weight of the unit, the mounting rating (structural load on the hardware), and the orientation of the equipment (inverted mounting). The following is a description of these factors.

Weight. The weight of the overall unit is needed to select the proper mounting bracket, but it is also a necessary factor when fastening the mounting bracket to a surface. All mounting brackets require either screws or bolts to mount to a surface.

Mounting Ratings.

(1) Equipment less than 13.6 kg (30 lb):
   (a) Wood fasteners should penetrate a minimum of 5.08 cm (2 in.) into the surface.
   (b) In concrete, use lead anchors or expansion bolts with at least 27.2 kg (60 lb) pull out strength.
   (c) In steel, use bolts long enough to accommodate a lock washer and nut.
(2) Equipment up to 36.3 kg (80 lb):
   (a) In wood, use 0.952 cm (⅜ in.) diameter bolts that should penetrate a minimum of 8.89 cm (3½ in.) into the surface.
   (b) In concrete, use lead anchors or expansion bolts with at least 68 kg (150 lb) pull out strength.
   (c) In steel, use 0.952 cm (⅜ in.) diameter bolts long enough to accommodate a lock washer and nut.

Inverted Mounting of Equipment. Most weight loads of the mounts, if used in a ceiling application, are reduced by a factor of 50 percent. Consult the manufacturers' specification sheets for specific requirements.

A.7.5.4 Such hardware can include tamper-resistant bolts, nuts, and screws, locks, and similar equipment.

A.7.7.1 Installers should know the low voltage codes and how to apply them according to their area of work. Knowledge of raceways should include the following as it applies to low voltage systems:

(1) Practices necessary for the installation of raceway
(2) Purpose of each raceway
(3) Tools required for the professional installation of raceway
(4) Restrictions of raceway

A.7.7.2.1.1 Underground/direct burial, pole to pole outside/UV protected, return air plenum/plenum rated, and so forth are examples of different insulation jackets.

A.7.7.2.3.2 The only acceptable connector should be a three-piece crimp connector consisting of a separate center tit, jacket sleeve, and main body that snaps onto the center tit and under the crimp sleeve and cable shield. The installer can come upon various pieces of equipment that require the termination of the coaxial cable to be something other than a BNC (i.e., F, UHF, RCA connectors, etc.). Only under these

circumstances, it should be the responsibility of the installer to use the appropriate connector as dictated by the equipment. Inline adapters should not be used.

A.7.8 The three applications for wiring within CCTV systems are as follows:

(1) Control
(2) Power
(3) Video signal transmission

A.7.8.1 The purpose of low voltage control cabling is to carry various low voltage signals to devices within the CCTV system. Such devices could include, but are not limited to, the following:

(1) Remote positioning devices (pan/tilt units, scanner units, domes)
(2) Cameras (primary input power)
(3) Zoom lenses
(4) Auxiliary devices (low voltage wipers and washers, low voltage heaters and blowers, remote relays)

A.7.8.3.1 It is understood that mini coaxial cable can be used for interconnection between devices within the control cabinet. In those applications where the cable exceeds its manufacturer's rated maximum, the installer can overcome the limitation by using a cable with less transmission loss or a different mode of transmission (e.g., fiber optics) or install an appropriate video amplification system.

A.7.9 Although RF is used for command/control of video systems and transmission of video images, it violates the definition of a closed system.

A.8.1.2.5 To minimize the unintentional operation of a portable device, factors such as jarring, contact with clothing, and similar sources should be considered.

A.8.2.2.8 Each employee expected to use a holdup alarm initiating device should be instructed that if they are directly confronted by the attacking party, they should not attempt to operate a holdup alarm initiating device. In addition, they should be trained to follow the procedures provided by their employer and the law enforcement agency having jurisdiction.

A.8.2.2.9 Off-premises locations that are used to receive holdup alarm signals should be equipped to retransmit signals to the law enforcement center that serves the property. Examples of off-premises locations that can receive holdup alarm signals are central stations that meet the requirements of UL 827, *Standard for Central-Station Alarm Services*.

A.8.3.2.5 The intent of a duress system is to notify onsite personnel of a potentially hostile civil disturbance or emergency at the protected property and for summoning assistance to the area of the civil disturbance or emergency.

A.8.4.2.1 To reduce the incidence of inadvertent ambush signals, the following steps should be taken:

(1) If an ambush feature is provided in a control unit that is also used to operate other systems, the default setting should be that it is disabled.
(2) An ambush signal should only be sent by a unique code.
(3) A control panel that is also used to operate other systems should not derive the ambush code from an existing operating code such as a "user code plus ambush digit" sequence.

A.8.4.2.1.1 Implementation of this feature can include, but is not limited to, any of the following:

(1) Simultaneous depression of two buttons where, if either of the buttons have multiple functions, the two buttons are nonadjacent
(2) If the cover protects only emergency function buttons, depression of a single button after lifting the cover that normally protects it
(3) Depression of a single button for at least 2 seconds

A.8.4.2.4 Each person that is expected to use an ambush alarm initiating device should be instructed to follow the procedures provided by the operator of the protected premises and the law enforcement agency having jurisdiction.

A.8.4.2.5 Off-premises locations that are used to receive ambush alarm signals should be equipped to retransmit signals to the law enforcement center that serves the property.

Examples of off-premises locations that can receive ambush alarm signals are central stations that comply with UL 827, *Standard for Central-Station Alarm Services*.

A.9.1 More stringent inspection, testing, and maintenance procedures that are required by other parties can be permitted.

A.9.1.3 Equipment performance can be affected by building modifications, occupancy changes, changes in environmental conditions, device location, physical obstructions, device orientation, physical damage, improper installation, degree of cleanliness, or other obvious problems that might not be indicated through electrical supervision.

A.9.1.4 The responsible party for the electronic premises security system is the individual or organization that ensures that inspection, testing, and maintenance are performed.

A.9.2.1 Examples of an indication can be a trouble signal to the control panel or controller, a reader that is not operating, a CCTV camera that is no longer providing an image, or other similar events.

A.9.2.2 These measures are temporary. Temporary mitigating measures should be considered by the owner or responsible party during impairments based on an assessment of the risk to the protected property or the occupants. Depending on the risk assessment, the AHJ can be consulted. The recommendations from the consultation should be implemented for the period that the system is impaired.

A.9.3.5.2(1) The factory training and certification should be specific and current to the equipment that is being used, and proof of this factory training and certification should be made available to the AHJ when requested.

A.9.3.6.1 In addition to advising the personnel within the protected premises that the system is being tested or maintained and that signals generated from the system(s) should not be acted upon, the owner or responsible party should be advised that the system or a part of the system may not be fully functional during the testing or maintenance procedure and that appropriate safeguards should be taken, based upon the perceived risk.

The owner or responsible party should also be informed that if the system is placed into a degraded mode, that some, if not all, information from those nodes can be lost during the time in which the node or nodes are down.