

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Users of NFPA codes, standards, recommended practices, and guides should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments.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

Chapter 1 Administration	731- 4	Chapter 6 Electronic Access Control Systems	731-15
1.1 Scope	731- 4	6.1 Fundamentals	731-15
1.2 Purpose	731- 4	6.2 Administration Tools/Interface	731-16
1.3 Application	731- 4	6.3 Network Interface Device	731-16
1.4 Retroactivity	731- 4	Chapter 7 Video Surveillance Systems	731-16
1.5 Equivalency	731- 4	7.1 General	731-16
1.6 Units and Formulas	731- 5	7.2 Cameras	731-16
Chapter 2 Referenced Publications	731- 5	7.3 Low-Level Lighting Conditions	731-16
2.1 General	731- 5	7.4 Enclosures	731-16
2.2 NFPA Publications	731- 5	7.5 General Hardware and Mounts	731-17
2.3 Other Publications	731- 5	7.6 Lens	731-17
2.4 References for Extracts in Mandatory Sections	731- 5	7.7 Physical Conductors	731-17
Chapter 3 Definitions	731- 5	7.8 Applications of Conductors	731-17
3.1 General	731- 5	7.9 Radio Frequency (RF). (Reserved)	731-17
3.2 NFPA Official Definitions	731- 5	Chapter 8 Holdup, Duress, and Ambush Systems	731-17
3.3 General Definitions	731- 6	8.1 General	731-17
Chapter 4 Fundamentals	731- 7	8.2 Holdup Alarm Systems	731-18
4.1 Application	731- 7	8.3 Duress Alarm Systems	731-18
4.2 Power Supplies	731- 7	8.4 Ambush Alarm Systems	731-18
4.3 System Functions	731- 9	Chapter 9 Testing and Inspections	731-19
4.4 Performance and Limitations	731- 9	9.1 Scope	731-19
4.5 Installation and Design	731- 9	9.2 Impairments	731-19
4.6 System Requirements	731-11	9.3 General Testing, Inspection, and Maintenance	731-19
4.7 Documentation	731-12	9.4 System Testing	731-19
4.8 Central Station Electronic Premises Security Systems	731-12	9.5 Inspection and Testing Frequency	731-25
Chapter 5 Intrusion Detection Systems	731-12	Annex A Explanatory Material	731-25
5.1 General	731-12	Annex B Camera Specifications	731-41
5.2 Exterior Detection Systems	731-13	Annex C Camera Selection	731-42
5.3 Interior Detection Systems	731-13	Annex D Informational References	731-43
5.4 Vaults and Safes	731-15	Index	731-44

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 sub-panels 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 non-alarm 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 re-sound 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 non-alarm 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.