# UL 2610

## STANDARD FOR SAFETY

Commercial Premises Security Alarm Units and Systems

UL Standard for Safety for Commercial Premises Security Alarm Units and Systems, UL 2610

Second Edition, Dated April 7, 2021

***Summary of Topics***

***This new edition of ANSI/UL 2610 dated April 7, 2021 contains several editorial changes, clarifications and technology updates.***

The revised requirements are substantially in accordance with Proposal(s) on this subject dated October 23, 2020 and January 27, 2021.

No Text on This Page

**APRIL 7, 2021**

**ANSI/UL 2610-2021**



# UL 2610

## Standard for Commercial Premises Security Alarm Units and Systems

First Edition – November, 2018

**Second Edition**

**April 7, 2021**

This ANSI/UL Standard for Safety consists of the Second Edition.

The most recent designation of ANSI/UL 2610 as an American National Standard (ANSI) occurred on April 7, 2021. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, and Title Page.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

No Text on This Page

## CONTENTS

### INTRODUCTION



### CONSTRUCTION

### ASSEMBLY



### FIELD WIRING CONNECTIONS

**INTERNAL WIRING**



**COMPONENTS, ELECTRICAL**



**SPACINGS**



**PERFORMANCE**



**OPERATION**

**COMMON TESTS**

## INSTALLATION AND OPERATING INSTRUCTIONS



## APPENDIX A Standards for Components

## APPENDIX B (Informative)

## INTRODUCTION

### 1 Scope

### 1.1 General

1.1.1 These requirements cover construction, performance, operation, and maintenance of:

a) Central station burglar alarm systems intended and specifically designated for burglary-protection use at mercantile and banking premises, mercantile safes and vaults, and bank safes and vaults;

b) Police station connected burglar alarm units and systems for use in mercantile premises, mercantile safes and vaults, and bank safes and vaults;

c) Local burglar alarm units and systems for use in mercantile premises, mercantile safes and vaults, and bank safes and vaults;

d) Proprietary burglar alarm units and systems;

e) Holdup alarm systems of the remote-station type intended for installation in banks, stores, cashiers' cages, pay offices, and the like.

f) Digital alarm communicator system units, interconnected to or integral, for use with central station burglar alarm systems, proprietary burglar alarm systems, police station-connected burglar alarm systems, and holdup alarm systems.

g) Power supplies used to provide electrical power and standby power for burglar-alarm equipment in accordance with the following:

1) The requirements of this standard;

2) The Standard for Access Control System Units, UL 294;

3) The Standard for Intrusion-Detection Units, UL 639;

4) The Standard for Household Burglar-Alarm System Units, UL 1023;

5) The Standard for Burglary-Resistant Electric Locking Mechanisms, UL 1034; and

6) The Standard for Antitheft Alarms and Devices, UL 1037.



### 1.2 Central station burglar alarm

1.2.1 A central station burglar alarm system consists of electrical protection circuits and devices that are transmitted automatically to, recorded in, maintained from, and supervised from a central (monitoring) station that employs trained operators and alarm investigators who are in attendance at all times and take appropriate action in response to a received signal.

1.2.2 These requirements serve as the basis of classification of central station burglar alarm system transmission methods, however, the requirements covering the complete systems are contained in the Standard for Central-Station Alarm Services, UL 827.

### 1.3 Police station connected burglar alarm

1.3.1 A police station connected alarm system consists of protective circuits and devices, connected through control apparatus to an optional sounding device mounted on an outside or inside wall of the

building in which the protected property is situated, and a constantly-manned police department or law enforcement center. The connection to a police department may be:

a) Direct, or

b) Through a central (monitoring) station complying with the Standard for Central-Station Alarm Services, UL 827.

1.3.2 Intrusion into or disturbance of the units or wiring causes the sounding device to be actuated (if applicable) and a signal to be transmitted to the police department. The sounding device and signal to the police department continue to operate until it is stopped by using the proper control key, by exhaustion of the power supply, or by action of an automatic timing element that is preset for a definite operating period.

1.3.3 The operation of a police station connected alarm system is partially under the control and domination of the owner or others interested in the property. However, it is required that police station connected systems be maintained under the care and regular inspection service of the installing company. The installing company is expected to respond promptly to troubles or calls for service on report of the owner or police department. It is the responsibility of the owner to switch the system on and off duty and to report malfunctioning of the system to the service company.

## 1.4 Local burglar alarm

1.4.1 A local alarm system consists of protective circuits and devices, connected through control apparatus to an enclosed tamper-protected sounding device mounted on an outside wall of the building in which the protected property is situated. Intrusion into or disturbance of the units or wiring causes the sounding device to be actuated. The sounding device continues to operate until it is stopped by using the proper control key, by exhaustion of the power supply, or by action of an automatic timing element that is preset for a definite operating period. Local mercantile burglar-alarm systems are intended for the protection of mercantile premises or mercantile safes and vaults. Local bank burglar alarm systems are intended for the protection of bank safes and vaults.

1.4.2 The operation of a local alarm system is partially under the control and domination of the owners or others interested in the property. However, it is required that systems be maintained under the care and regular inspection service of the installing company. The installing company is expected to respond to troubles or calls for service promptly on report of the owner. It is the responsibility of the owner to switch the system on and off duty and to report malfunctioning of the system to the service company.

## 1.5 Proprietary burglar alarm

1.5.1 A proprietary burglar alarm system as referred to by these requirements is a system in which alarm initiating circuits and devices are installed at a property and are connected directly or indirectly to constantly monitored receiving equipment at a proprietary (monitoring) station. The proprietary (monitoring) station is located at the protected property and intended for operation by personnel responsible to the owner of the protected property.

1.5.2 The protected property may consist of a single property or of noncontiguous properties under a single ownership. The system is arranged so that a predetermined change in the alarm initiating circuits or devices automatically causes transmission of an alarm signal over a supervised signaling channel to the proprietary (monitoring) station.

1.5.3 Proprietary burglar alarm units and systems are also specially designated as to their intended use on mercantile premises, mercantile safes and vaults, and bank safes and vaults.

## 1.6 Holdup alarm

1.6.1 Holdup alarm systems of the remote-station type intended for installation in banks, stores, cashiers' cages, pay offices, and the like, are to provide a means of transmitting a silent call for help in the event of interior robbery.

1.6.2 A holdup alarm signal shall be transmitted directly to a constantly-manned police station equipped for broadcasting radio calls to cruising squad cars or to a central (monitoring) station with facilities for relaying calls to a law enforcement agency with such broadcasting facilities. The central (monitoring) station shall comply with the Standard for Central-Station Alarm Services, UL 827.

## 1.7 Digital alarm communicator units

1.7.1 The operation of a digital alarm communicator system is under the control of the owner or others interested in the property, and/or the operators at the monitoring station. A need for off-premises transmission will activate the digital alarm communicator transmitter that contacts a digital alarm communicator receiver located at a monitoring station through the telephone company's switched network (dial system) and transmits a message identifying the change in condition at the protected premises.

1.7.2 A digital alarm communicator system may be classified as police station-connected if:

a) It is used in combination with a protected premises control unit, an optional alarm sounding device, and an alarm housing that complies with this standard; and

b) The signals are transmitted to a digital burglar-alarm communicator receiver located at a central station that complies with Standard for Central-Station Alarm Services, UL 827.

## 1.8 Burglar alarm power supplies

1.8.1 These requirements cover power supplies for use as components in burglar-alarm system units. The input ratings of power supplies covered by these requirements are not more than 300 volts and the output ratings are low-voltage, power-limited. See 6.19(c). Power supplies integral with a burglar alarm system unit, or separate power supplies intended for use with a specific unit, are covered in the applicable sections of this standard. These requirements may also be covered by the standards specified in 1.1.1(g), as applicable.

1.8.2 Police station connected burglar alarm units, local burglar alarm units, proprietary burglar alarm units, central station burglar alarm units, and digital alarm communicator system units, contain requirements for attack resistance against a power supply providing energy to a local audible alarm sounding device or to a device that will transmit a signal from the protected area to a remote location, such as a central (monitoring) station or police station. A power supply complying with the requirements of this standard that is to be used for any of these purposes shall be capable of being mounted inside an enclosure that will provide the required attack resistance, or shall be provided with an enclosure that will provide the required attack resistance. See Section 67 to determine the attack resistance requirements that will apply.

1.8.3 These requirements do not cover power supplies for use at a central (monitoring) station. Such power supplies are covered by the Standard for Central-Station Alarm Services, UL 827. These requirements do not cover power supplies for use in hazardous locations, as defined in the National Electrical Code, NFPA 70. These requirements do not cover power supplies covered by the Standard for Power Units Other Than Class 2, UL 1012, or battery chargers covered by the Standard for Battery Chargers for Charging Engine-Starter Batteries, UL 1236.

## 1.9 Common requirements

1.9.1 Protective devices installed on individual properties are further classified as to extent of protection at each location. Requirements covering installation and classification (of extent) of alarm protective equipment at individual locations are published in the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, which is intended to be referenced by burglar-alarm installers.

1.9.2 If equipment covered by these requirements is intended for use in a combination burglar-alarm and fire-protective signaling system, the portion of the equipment serving a fire-alarm function is covered by the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, or the Standard for Household Fire Warning System Units, UL 985.

1.9.3 These systems usually operate within the limits of Class 2 remote control and signal circuits as defined by Article 725 of the National Electrical Code, NFPA 70.

1.9.4 A system that provides line security may be classified as either Standard Line Security or Encrypted Line Security. See Standard Line Security Equipment, 40.14, and Encrypted Line Security Equipment, 40.15.

1.9.5 Equipment used in a burglar alarm system shall comply with the requirements for that product and shall not be modified before, during, or after installation into the system, except for software/firmware upgrades as noted in Section 38.

1.9.6 Products intended for use in air-handling spaces in Accordance with Section 300.22, (C) of the National Electrical Code, NFPA 70, are additionally investigated to the Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces, UL 2043.

1.9.7 For equipment utilizing power over communications cables, refer to Section 36, Power Over Communications Cable Equipment. Compliance with the Standard for Ethernet, IEEE 802.3 (at or af) specifications shall not be verified as part of these requirements. Refer to Appendix B.

## 2 Components

2.1 Except as indicated in 2.2, a component of a product covered by this standard shall comply with the requirements for that component. See Appendix A for a list of standards covering components generally used in the products covered by this standard.

2.2 A component is not required to comply with a specific requirement that:

a) Involves a feature or characteristic not required in the application of the component in the product covered by this standard; or

b) Is superseded by a requirement in this standard.

2.3 A component shall be used in accordance with its rating established for the intended conditions of use.

2.4 Specific components are incomplete in construction features or restricted in performance capabilities. Such components are intended for use only under limited conditions, such as certain temperatures not exceeding specified limits, and shall be used only under those specific conditions.

## 3 Units of Measurement

3.1 Values stated without parentheses are the requirement. Values in parentheses are explanatory or approximate information.

3.2 Unless otherwise indicated, all voltage and current values mentioned in this standard are root-mean-square (rms).

## 4 Undated References

4.1 Any undated reference to a code or standard appearing in the requirements of this standard shall be interpreted as referring to the latest edition of that code or standard.

## 5 Terminology

5.1 The term "product" as used in this standard refers to all types of units and systems for all burglar alarm applications noted.

## 6 Glossary

6.1 For the purpose of this standard, the following definitions apply.

6.2 ACKNOWLEDGMENT SIGNAL – An audible and/or visual signal that is sent to the subscriber by the monitoring station to notify the subscriber that the closing signal has been received, indicating that the protection system has been properly armed. The acknowledgment signal can be sent manually or automatically. Also referred to as "Ringback".

6.3 ADMINISTRATOR – An authorized entity that is in possession of the credentials necessary for the ability to perform an upgrade to a control unit's software and/or firmware.

6.4 AIR-HANDLING SPACE – Space not specifically fabricated for environmental air-handling purposes but used for air handling purposes as a plenum. (The space above a hung ceiling used for environmental air-handling is an example.)

6.5 ALARM INITIATING DEVICE – A device whose operation results in a burglar alarm signal at the control unit. Examples of alarm initiating devices are motion sensors, door/window contact switches, glass break detectors, or the like.

6.6 ALARM SIGNAL – An audible signal indicating a burglar alarm condition requiring immediate action, such as an alarm initiated from an intrusion detector, door switch, floor mat, or the like.

6.7 ALARM SOUNDING DEVICE – An audible signal appliance (bell, horn, siren, or speaker) complying with the requirements in the Standard for Audible Signal Appliances for General Signaling Use, UL 464, and this standard, that is used to signal unauthorized entry or attempted entry into a protected area or object.

6.8 ALARM SOUNDING DEVICE HOUSING – A housing, or the equivalent, that is used to protect an alarm sounding device from being silenced by physical attack. Also see Alarm Sounding Devices, 11.11. There are two versions:

a) Outside – A housing intended to be located outside of the protected area.

b) Inside – A housing intended to be located within the protected area where it can be seen by an intruder.

6.9 ALARM SYSTEM – Protective system consisting of control units, alarm initiating devices, alarm sounding devices, and off-premises communication devices, which emit and transmit remote and local notification of alarm and/or trouble conditions occurring at the protected premises.

6.10 ANNUNCIATOR – A unit containing one or more indicator lamps, alphanumeric displays, computer monitors, audible indicators, or other equivalent means in which each indication provides status information about a circuit, condition, system, or location.

6.11 ARM – The act of turning on the burglar alarm system and setting the protective circuits.

6.12 ARMING STATION (KEYPAD) – A means for manually arming, disarming, or controlling the alarm system. Provided with a visual-indicating device containing identified targets or indicator lamps, alphanumeric displays, audible indicators, or other equivalent means, in which each indication provides status information about a circuit, condition, and/or location.

6.13 AUTOMATION SYSTEM – A computer system that consists of hardware and software components, including the alarm-monitoring software, the operating system, and programming languages, required to make the system operational. An automation system may be configured as a computer system that is directly connected to hardware-based central-station receivers, software-based receivers, or is connected to remote receivers located in central stations other than the one where the automation system is located. It is used to automatically process change-of-status signals such as trouble, supervisory, opening (disarming) and closing (arming), and similar signals that it receives from the central station receiving equipment. Automation systems shall comply with the requirements in the Standard for Central-Station Automation Systems, UL 1981.

6.14 BANK SAFE AND VAULT ALARM SYSTEM – Burglar alarm system located in a bank or financial institution which includes protection for a safe and/or vault.

6.15 BASIC INSULATION – The insulation applied to live parts to provide basic protection against the risk of electric shock. Basic insulation does not necessarily include insulation used exclusively for functional purposes. See also the Standard for Double Insulation Systems for Use in Electrical Equipment, UL 1097.

6.16 BIOMETRICS – Authentication of human physical characteristics used to identify an individual.

6.17 CENTRAL STATION – A physically protected building, distributed group of buildings, or an enclosed area within a building, whose ownership is not the same as that of the property (ies) being monitored, that is manned for the purpose of providing immediate attention to defined signals received from the protected property (ies). Also referred to as "Central Station", "Central Supervising Station", "Monitoring Station", or the like.

6.18 CHECK-IN SIGNAL – A signal that is periodically sent by the control unit/communicator to verify that the transmission equipment at the protected property, and the communication path, are operational. A unique signal that is initiated at a pre-established frequency, or an opening, closing, or any other signal sent by the alarm system that occurs within the pre-established frequency, may serve as a check-in signal.

6.19 CIRCUITS, ELECTRICAL:

a) High-Voltage – A circuit involving a potential of not more than 600 volts and having circuit characteristics in excess of those of a low-voltage power limited circuit.

b) Low-Voltage – A circuit involving a potential of not more than 30 volts AC rms, 42.4 volts DC, or AC peak.

c) Power Limited – A circuit whose output is limited as specified in Article 725 of the National Electrical Code, and as noted in Table 45.1 and Table 45.2. The power limitation shall be provided by the construction of the transformer, a fixed impedance, a non-interchangeable fuse, a nonadjustable manual reset circuit protective device, or a regulating network.

d) Power over Communications Cable – A limited energy circuit that meets the requirements of Section 36.

e) Risk of Electric Shock – A risk of electric shock is determined to exist within a circuit unless that circuit meets the following criteria:

1) The circuit is supplied by an isolating source such that the maximum open-circuit voltage potential available to the circuit is not more than 30 V AC rms, 42.4 V DC, or 42.4 V peak; and

2) The circuit is supplied by an isolating source such that the current available through a 1500-ohm resistor connected across any potential in the circuit (including to ground) does not exceed 0.5 mA.

3) A limited energy, power over communications circuit that meets the requirements of Section 36.

f) Risk of Fire – A risk of fire is considered to exist at any two points in a circuit where:

1) The open circuit voltage is more than 30 V AC rms, 42.4 V DC, or 42.4 V peak, and the energy available to the circuit under any condition of load including short circuit, results in a current of 8 A or more after 1 minute of operation; or

2) A power of more than 15 watts can be delivered into an external resistor connected between the two points.

*Exception: The product meets all of the requirements of Section 36 for equipment utilizing power over communications cables.*

6.20 CLOSING SIGNAL – The transmission sent to the monitoring station upon the act of turning on (arming) the burglar alarm system and setting the protective circuits. This signal represents "closing" the business for the day.

6.21 CODE TRANSMITTER SYSTEM – A communication system, such as McCulloh, that provides for the connection of more than one protection system to a single alarm receiving unit at the monitoring station. The code transmitter sends a coded signal to the monitoring station, repeated not less than three times, if the subscriber's protective circuit is disturbed by an intrusion or unauthorized opening.

6.22 COMMUNICATION CLOUD – The area in the communication path that is supported by providers of communication services in which signals travel between a protected property and a monitoring station. Depending on the type of transmission that is used, signals may travel on a single defined route or through various routes depending upon availability when the signal is initiated.

6.23 COMPUTER SYSTEM, FAULT TOLERANT – A computer system containing multiple power supplies, disk drives, processors, and controllers, each backing up and checking on the processes of others. In the event of a component failure, the other modules take over the function performed by the failed components without affecting the operation of the computer. In addition to the duplicating hardware, a fault-tolerant system includes the necessary software components consisting of the operating system, programming languages, and the alarm monitoring software required to make the system operational. A fault-tolerant computer system is considered to be redundant.

6.24 COMPUTER SYSTEM, REDUNDANT – Two or more computer systems maintained at a monitoring station, either of which can be quickly connected and operational for handling alarm signals in the event that the other computer fails to operate. See 6.23 for the definition of a fault-tolerant computer system. A fault-tolerant computer system is considered to be redundant.

6.25 CONTIGUOUS PROPERTY – A single owner or single user on a continuous plot of ground, including any buildings thereon, that is not separated by a public thoroughfare, transportation right-of-way, property owned or used by others, or body of water not under the same ownership.

6.26 CONTROL UNIT – A unit that directly or indirectly monitors the status of initiating devices, processes any status-change signals, and performs logical control to generate output signals and/or off-premises communication as required by the system type.

6.27 CONTROL UNIT ACCESSORY – A device or appliance externally connected to a control unit that is employed to assure the intended operation of a system or to provide supplementary signaling, annunciation, or both. Examples of control unit accessories are: annunciators, auxiliary relays, end-of-line resistors or diodes, keypads, or remote switches.

6.28 CONTROL UNIT SYSTEM TYPES:

a) Central Station – A system for use with mercantile premises, mercantile safes and vaults, and bank safes and vaults, in which status-change signals at a protected premises are automatically transmitted to a central (monitoring) station where competent and experienced personnel take appropriate action in response to a received signal. The central (monitoring) station is controlled and operated by a person, firm, or corporation whose business includes the furnishing, maintaining, or monitoring of supervised burglar alarm systems.

b) Holdup – Holdup alarm systems of the remote-station type are intended for installation in banks, stores, cashiers' cages, pay offices, and the like, to provide a means of transmitting a silent call for help in the event of interior robbery. Holdup alarms are dispatched upon immediately without the need for any type of alarm verification.

c) Local – A system for use with mercantile premises, mercantile safes and vaults, and bank safes and vaults, which indicates alarm and trouble conditions via alarm sounding devices located at the protected premises.

d) Police Station Connected – A system for use with mercantile premises, mercantile safes and vaults, and bank safes and vaults, in which status-change signals are automatically transmitted to a constantly-manned police station where police authorities take appropriate action in response to a received signal, or to a constantly-manned law enforcement center which dispatches to a police station.

e) Proprietary – A system installed at the protected premises in which status-change signals occurring at the protected premises are automatically transmitted to a constantly manned, on-premises proprietary (monitoring) station where trained, competent personnel take appropriate action in response to a received signal. The protected property may be contiguous or noncontiguous but must be under a single ownership.

6.29 CORD-CONNECTED UNIT – A unit intended for connection to the power source by means of a supply cord. Such a unit is intended to be moved for reasons of interchange or realignment of the units of a system.

6.30 CREDENTIAL – A mechanism that defines or distinguishes the identity of an entity (e. g. a password, PIN, or biometric means).

6.31 CRITICAL COMPONENT – A critical component is one whose malfunctioning will impair the normal operation of the product, or create a risk of fire or electrical shock.

6.32 CROSS ZONING – A means of installing and programming the burglar alarm system in such a way that two or more zones are interdependent in creating an alarm condition. The control panel will not annunciate and/or send an alarm to the monitoring station unless the system detects an alarm condition from two or more zones in a particular area within a preset time window.

6.33 CRYPTOGRAPHIC AUTHENTICATION – Algorithms intended to ensure the secrecy and/or authenticity of messages.

6.34 DEAD METAL PART – A metal or other electrically conductive part, accessible or inaccessible, that is not conductively connected to a live part.

6.35 DIGITAL ALARM COMMUNICATOR RECEIVER (DACR) – A unit located at a monitoring station that will receive and display signals from a digital alarm communicator transmitter (DACT).

6.36 DIGITAL ALARM COMMUNICATOR SYSTEM (DACS) – A system in which signals are transmitted from a digital alarm communicator transmitter (DACT), by cellular and/or telephone landline transmission, to a digital alarm communicator receiver (DACR) located at the monitoring station.

6.37 DIGITAL ALARM COMMUNICATOR TRANSMITTER (DACT) – A unit located at the protected premises that will contact the digital alarm communicator receiver (DACR) through the public switched telephone network. The DACT seizes the connected telephone line, dials a pre-selected number to connect to a DACR, and transmits the necessary data to identify the DACT and the change of status at the protected premises. As covered by these requirements, the DACT either:

a) Provides all alarm or monitoring control functions; or

b) Interfaces with an alarm or monitoring control unit that provides this function (a slave unit).

6.38 DISARM – The act of turning off the burglar alarm system so that it will no longer annunciate an alarm event (unless a particular circuit is programmed as a "24-hour zone").

6.39 DURESS ALARM – A silent alarm signal generated by the manual entry of a designated code at the system keypad in the event that the user needs assistance, such as when being forced to disarm the burglar alarm system against the user's will to enter the premises. Duress alarms are typically treated as holdup alarms by monitoring station personnel and are dispatched upon immediately without the need for any type of alarm verification.

6.40 ENCRYPTION – The process of transforming information/data using an algorithm to make it unreadable to anyone except those authorized, usually referred to as a key.

6.41 END-OF-LINE DEVICE – A device installed at the end of a circuit for the purpose of monitoring the circuit for fault conditions.

6.42 ENDSPAN – A device that is typically a network switch capable of supplying power over a communications circuit.

6.43 ENTITY – Person, device, and/or appliance or service which interacts with a control unit.

6.44 ENTRY/EXIT DELAY – A time delay on an entry/exit zone of a burglar alarm system that enables the user to enter the protected premises and disarm the system, or arm the system and exit the protected premises, without creating an alarm condition.

6.45 ETHERNET CABLING – A structured cabling system using 4 pair unshielded or shielded twisted pair cable, meeting Category 5e performance or higher and conforming to the Standard for Balanced Twisted-Pair Telecommunications Cabling and Components, ANSI/TIA-568C.2, requirements. The extent of the cabling is taken to be the channel that connects the appropriate port of the network switch to the powered device.

6.46 EVENT LOG – A comprehensive data record, maintained at the monitoring station and/or control unit, of the events that are associated with remote access.

6.47 FALSE ALARM – An annunciation and/or transmission by the burglar alarm system indicating the occurrence of an alarm condition when no evidence of an actual alarm event is found.

6.48 FAULT – An open, ground, or short-circuit condition on any line extending from a product.

6.49 FIELD WIRING – Conductors to be installed by qualified personnel to connect a product to source(s) of supply, devices, other products, and loads.

6.50 FIRMWARE – A software program or set of instructions programmed on a hardware device (e.g. Flash ROM, EPROM).

6.51 FIXED EQUIPMENT – A device intended to be permanently connected electrically.

6.52 GROUND FAULT – A circuit impedance to ground sufficient to result in the annunciation of a trouble condition.

6.53 HANDSHAKE SIGNAL – For Digital Alarm Communicator Systems (DACS), upon the occurrence of an event requiring off-premises signaling, the phone line is seized and automatically dials the monitoring station receiver. Upon answering, the receiver sends out a special tone ("handshake") which lets the DACT know that the DACR is ready to receive data transmission.

6.54 HARDWARE – Physical equipment that constitutes the components of a burglar alarm system.

6.55 HARDWARE KEY DEVICE – A mechanical or electronic device employed to enable the remote programming mode.

6.56 HOLDUP ALARM INITIATING DEVICE – A switch operated by hand or foot, by key, by removal of currency bills, or by other means to initiate a holdup alarm signal.

6.57 HOLDUP ALARM – A silent alarm generated by the manual or semiautomatic activation of a designated device intended to signal a robbery in progress. Holdup alarms are dispatched upon immediately without the need for any type of alarm verification.

6.58 HOSTED CENTRAL STATION – A hosted central station consists of services not limited to the storage of data from alarm monitoring software, data center equipment co-location, housing the automation system running alarm monitoring software, housing the receivers and automation system, or any combination thereof. Hosted central stations shall comply with the requirements of the Outline of Investigation for Hosted Central Station Services, UL 827A, the Standard for Central-Station Services, UL 827, and/or the Standard for Central-Station Automation Systems, UL 1981, as appropriate.

6.59 HVAC SYSTEM – Heating, Ventilating, and Air-Conditioning system.

6.60 INTERIOR ZONE – A protective circuit connected to a sensing device, such as a motion detector, which only monitors the interior of the premises.

6.61 KISS-OFF SIGNAL – For Digital Alarm Communicator Systems (DACS), after the monitoring station receives the transmission data, it sends a sign-off tone ("kiss-off") to the DACT to end the call and release the phone line.

6.62 LINE SECURITY, ENCRYPTED – In addition to Standard Line Security as noted below, Encrypted Line Security utilizes encryption algorithms with a minimum of 128 bits of security strength to provide data protection against a compromise attempt. Also see Encrypted Line Security Equipment, 40.15.

6.63 LINE SECURITY, STANDARD – Methods of supervising the communication channel used to transmit signals between the protected premises and the monitoring station. This supervision serves to detect compromise attempts on the communication channel that are intended to prevent signals from being annunciated at the monitoring station and which may allow entry into the protected premises without initiating a signal at the monitoring station. Also see Standard Line Security Equipment, 40.14.

6.64 LINE VOLTAGE – The voltage at any field connected source of supply, nominally 50 – 60 hertz, and either 115, 208, or 230 volts.

6.65 LIVE PART – A part:

a) That is conductively connected either:

1) To the power-supply circuit; or

2) To a secondary circuit that operates at more than 42.4 volts peak with reference to ground or accessible metal; and

b) In which the available current measured through a 1500-ohm resistor shunted with a 0.15-μF capacitor connected from the part to ground or to any other accessible part exceeds 0.25 mA.

6.66 LOCAL ALARM – An alarm annunciation at the protected premises caused by activation of an alarm sounding device.

6.67 LOCAL AREA NETWORK (LAN) – A combination of personal computers, servers, and communication devices that are connected to share data files, resources and applications located in close proximity, such as on the same floor or in the same or nearby building(s).

6.68 LONG-RANGE RADIO-FREQUENCY DEVICES – Any device that communicates between a protected premises and a monitoring station, subsidiary station, or another protected premises using a private radio network.

6.69 MANAGED FACILITIES-BASED VOICE NETWORK (MFVN) – A physical facilities based network capable of transmitting real-time packet switched data network (PSDN) signals with unchanged formats, that is managed, operated, and maintained by the service provider to ensure service quality and reliability from the subscriber location to public switched telephone network (PSTN) interconnection points or other MFVN peer networks. Also referred to as "Voice over IP (VoIP)".

6.70 MERCANTILE PREMISES SYSTEM – Burglar alarm system located in a place of business primarily under the control of the owner or others interested in the property.

6.71 MERCANTILE SAFE AND VAULT SYSTEM – Burglar alarm system located in a mercantile establishment which includes protection for a safe and/or vault.

6.72 MESSAGE(S) – Communicated data that contains specific information relating to the product and is transmitted via a wired or wireless pathway from an origin to a destination.

6.73 MIDSPAN – A midspan device is Power Sourcing Equipment (PSE) that injects power onto communications cable. It is located between the network switch and the Powered Device (PD).

6.74 MONITORING STATION – Term used throughout the standard to represent one of more of the following applications: Central Station (see 6.17), Police Station (see 6.89), or Proprietary Station (see 6.99).

6.75 MULTIPLEXING – A signaling method using wire path, cable carrier, radio, or combinations of these methods characterized by the simultaneous and/or sequential transmission and reception of multiple signals in a communication channel including means for positively identifying each such signal.

6.76 NETWORK SWITCH – Active electronic equipment that selects a path or circuit for sending a unit of data to its next destination.

6.77 NORMAL STANDBY CONDITION – The ready-to-operate condition of the product existing prior to its being tripped or operated by an intrusion.

6.78 OFF-HOOK – The condition in which a connection has been established with the Public Switched Telephone Network (PSTN) in preparation for dialing a telephone number.

6.79 ON-HOOK – The condition causing the equipment to disconnect from (hang up) the Public Switched Telephone Network (PSTN).

6.80 ONE-WAY RADIO (RF) – A system in which alarm system signals are transmitted from a radio alarm transmitter through a radio channel to at least two independently-powered, independently-operating, and separately-located radio repeaters or radio alarm monitoring station receivers, or by one of each. At least two separate paths shall be provided from the radio alarm transmitter to the ultimate radio alarm monitoring station receiver.

6.81 OPEN CIRCUIT FAULT – A circuit impedance increase sufficient to prevent normal operation.

6.82 OPENING SIGNAL – The transmission sent to the monitoring station upon the act of turning off (disarming) the burglar alarm system and protective circuits. This signal represents "opening" the business for the day.

6.83 PACKET SWITCHED DATA NETWORK (PSDN) – A type of data transmission in which data is divided into packets, each of which has a destination address. Each packet is then routed across a computer network. A packet may travel a different route than packets related to it. Internet Protocol (IP), Global System for Mobile (GSM), and General Packet Radio Service (GPRS) are examples of PSDN technology.

6.84 PANIC ALARM – An alarm generated by the manual activation of a designated device intended to signal a response to a threat. Panic alarms are dispatched upon immediately after alarm verification by the monitoring station.

6.85 PARTITION – Segmented section of a burglar alarm system that can be armed and disarmed independent of other areas, but operated under a single system control.

6.86 PERIMETER ZONE – A protective circuit connected to a sensing device, such as a door/window contact switch, which monitors an entry point of the protected premises.

6.87 PLAINTEXT – A character representation that is plainly readable as text and not masked and/or hidden.

6.88 POLICE DEPARTMENT – Any local or government-related law enforcement agency.

6.89 POLICE STATION – A physically protected building, distributed group of buildings, or an enclosed area within a law enforcement agency, that is constantly manned by police authorities for the purpose of providing immediate attention to defined signals received from the protected property(ies).

6.90 POLLING DATA LOOPS – An installation wiring circuit in which each device or component of an alarm system that is attached to the loop is polled to verify the continuity of the circuit.

6.91 POLLING SIGNAL – A signal that is periodically sent by the central/proprietary (monitoring) station to verify that the protected premises communication equipment, and the communication path, are operational.

6.92 PORTABLE EQUIPMENT – Cord- and plug-connected equipment that is capable of being carried or moved about.

6.93 POWER INJECTOR (INJECTOR/POWER BRICK) – Power sourcing equipment (PSE) similar to a midspan device, comprising three ports. These are:

a) Data in, typically from the network switch,

b) Data and power – nominal 48 or 53 VDC out, and

c) Line voltage from a utility supply.

6.94 POWER OVER COMMUNICATIONS CABLES – A means to supply DC power to a network device over communications cabling. The power supplied to the device may or may not be on the same conductors supporting data. Typical technologies include PoE (see Appendix B) and USB.

6.95 POWER SOURCING EQUIPMENT (PSE) – The power supply that provides DC power to the powered device (PD) through the communications cabling. It may be an endspan device, such as an enabled network switch, or a midspan device that is located in between the network switch and the powered device.

6.96 POWERED DEVICE (PD) – A device that receives DC power from the power sourcing equipment (PSE) through communications cabling. Also referred to as the load.

6.97 PRIMARY BATTERY – Any battery which, by design or construction, is not intended to be recharged.

6.98 PRIMARY POWER – Power provided by a commercial source available at the protected premises.

6.99 PROPRIETARY STATION – A physically protected building, distributed group of buildings, or an enclosed area within a building, having the same ownership as that of the properties being monitored, that is constantly manned for the purpose of providing immediate attention to all signals received from the protected areas and/or property (ies). Also referred to as "Central Supervising Station", "Central Supervisory Station", or the like.

6.100 PROTECTED PREMISES – Any building or part of a building that has a complete physical boundary. Examples of premises include stores, banks, offices, manufacturing facilities, warehouses, lofts, and stockrooms, and similar locations, used for the storage, manufacturing, sale, or handling of merchandise, valuables, and the like.

6.101 PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) – An assembly of communications equipment and telephone service providers that may utilize Managed Facilities-Based Voice Networks (MFVN) to provide the general public with the ability to establish communications channels via discrete dialing codes. (Source NFPA 72, 2010 edition).

6.102 RADIO FREQUENCY – Electromagnetic radiation, nominally above 20 kilohertz.

6.103 REINFORCED INSULATION – An improved basic insulation with such mechanical and electrical qualities that it, in itself, provides the same degree of protection against the risk of electric shock as double insulation. It may consist of one or more layers of insulating material. See, also, the Standard for Double Insulation Systems for Use in Electrical Equipment, UL 1097.

6.104 REMOTE ACCESS – The act of accessing a control unit at a distance from the protected premises, whereby the user does not have visual contact of the premises. Key FOB's are not included in this definition because they are intended to be used when in visual contact with the protected premises and are very limited in the distance they may be used.

6.105 REMOTE COMMUNICATION – Data exchange in which information is exchanged between the control unit and an authorized entity. Information exchanges such as remote monitoring, remote interaction, and software downloading would be considered remote communication.

6.106 REMOTE OPERATION – The function or actuation of the protected premises control unit via remote communication.

6.107 RESET – A control function that attempts to return a system or device to its Normal Standby Condition or non-alarm state.

6.108 SAFETY CIRCUIT – Any primary or secondary circuit that is relied upon to reduce the risk of fire, electric shock, or unintentional contact with moving parts that may cause injury to persons (an interlock circuit, for example).

6.109 SATELLITE/SUBSIDIARY STATION – A normally unattended physically secure facility linked by communication channels to a central (monitoring) station. Signals from protected properties are transmitted to the subsidiary station and then relayed to the central (monitoring) station. If the communication link between the subsidiary station and the central (monitoring) station is out of service, the subsidiary station can be staffed and operated as a central (monitoring) station.

6.110 SECONDARY BATTERY – Any battery which, by design or construction, is intended to be recharged.

6.111 SECONDARY/STANDBY POWER – Power provided from a secondary source, such as a battery, upon the loss of primary power.

6.112 SHORT CIRCUIT FAULT – A short circuit (wire-to-wire) fault is determined to be a resistance of 0.1 ohm or less across the circuit.

6.113 SHORT-RANGE RADIO-FREQUENCY DEVICES – Any device that communicates with control/receiving equipment at the protected premises by low-power radio signals in accordance with the Code of Federal Regulations (CFR) 47, Part 15.

6.114 SOFTWARE – Programs, instructions, procedures, data, and the like that are temporarily or permanently stored in the computer's memory or central processing unit (CPU) of a product, and are used to provide function and control of the computer's components, or are executed by the CPU of a product to influence the functional performance of that product.

6.115 SOFTWARE-BASED RECEIVING EQUIPMENT – Software packages that are installed in UL 60950-1 or UL 62368-1 evaluated Information Technology Equipment (ITE) network servers, configured to store messages in a compatible database. The software and hardware combination is intended to serve the same function as a traditional dedicated hardware receiving unit at the monitoring station. The software supports all of the signal-receiving, -recording and -supervision functions necessary for the normal operation of the associated subscriber's control units installed within a protected property.

6.116 STATIONARY EQUIPMENT – Cord- and plug-connected equipment that is intended to be fastened in place, or located in a dedicated space.

6.117 SUBSCRIBER – The user of the premises or item protected by a burglar alarm system. An authorized representative of the user may also be considered a subscriber.

6.118 SUPPLEMENTARY INSULATION – An independent insulation provided in addition to the basic (formerly functional) insulation to protect against the risk of electric shock in case of mechanical rupture or electrical breakdown of the basic insulation. An enclosure of insulating material may form a part or the whole of the supplementary insulation. See, also, the requirements for the Standard for Double Insulation Systems for Use in Electrical Equipment, UL 1097.

6.119 SYSTEM DATABASE – Information entered into the computer by authorized personnel including items such as, but not limited to, names, addresses, telephone numbers, security information for system users, graphics and the like.

6.120 TRANSMISSION METHODS – Any of the following communication methods: code transmitter, DACT (telephone line, cellular, or MFVN), multiplex, one-way radio (RF), packet switched data network, or two-way radio (RF).

6.121 TRANSMISSION PATH, DUAL – Communication signals from a protected property to a remote monitoring station are sent by different transmission techniques, which pass through separate demarcation points as they leave the protected property.

6.122 TRANSMISSION PATH, SINGLE – Communication signals from a protected property to a remote monitoring station are sent by a single transmission technique and pass through a single demarcation point as they leave the protected property.

6.123 TRANSMISSION PATH (SINGLE/DUAL), ALTERNATE PRIMARY – A method of activating one or more transmission paths to maintain the same level of supervision without interruption.

6.124 TROUBLE SIGNAL – A visual or audible signal indicating a fault condition of any nature, such as an open circuit, ground fault or other trouble condition, occurring in the product or connected wiring.

6.125 TRUSTED PHYSICAL PATH – A contiguous and direct path for communications constructed of physical media. A directly connected crossover network cable, USB cable, or vendor approved cable would be considered a trusted path.

6.126 TWO-WAY RADIO (RF) – A system in which alarm system signals are transmitted and received through a radio channel between a radio alarm transmitter/receiver and a radio alarm monitoring station. The signals may or may not be relayed through a radio repeater. A two-way radio system shall be considered as a multiplex system.

6.127 UNINTERRUPTIBLE POWER SUPPLY (UPS) – Equipment that will continue to provide alternating current (AC) power to a load in the event of failure of the normal AC power source. A UPS may also provide a more constant voltage and frequency supply to the load. When the normal source of AC fails, the UPS is powered by a DC source from batteries, an uninterruptible battery system (UBS), or both.

6.128 USER – A person who has authorized access to the control unit or system.

6.129 USER VALIDATION – The act of an electronic device, upon the input of "user credentials", validating that the credentials are legitimate, allowing the user to proceed to access the system, or upon failure to match the credentials, deny access to the system.

6.130 WIDE AREA NETWORK (WAN) – A WAN differs from a LAN in that a WAN makes data connection across a broad geographic area. Companies use a WAN to connect to various company sites so that information can be exchanged between distant offices.

6.131 ZONE – A defined area within the protected premises from which a status indication can be received or an area in which control can be executed.

## 7 Information Required for Assessment

7.1 The following documentation shall be required as applicable to determine compliance, and shall be furnished with the sample(s) submitted for investigation:

a) Installation and operating instructions intended to accompany each product or component as produced (see Section 91);

b) Schematic diagrams of all circuits;

c) Printed wiring board construction drawings (e.g. component layouts, foil patterns);

d) Bill of Materials (BOM)/parts list (including manufacturer name and part number for critical components);

e) Mechanical drawings; and

f) Markings to be applied to the product as required in Markings, Section 89.

## 8 Version Number

8.1 If reprogrammable, a unit, system, or equipment shall provide some method to identify the current version of the software, firmware, and/or programming logic code being used. Subversions that are used to distinguish non-critical logic changes are not required to be identified. This information shall also appear in the product installation instructions.



# CONSTRUCTION

# ASSEMBLY

## 9 General

### 9.1 Specific product requirements

9.1.1 Products that currently meet all the requirements of the Standard for Information Technology Equipment – Safety – Part 1: General Requirements, UL 60950-1, or the Standard for Audio/Video, Information and Communication Technology Equipment – Part 1: Safety Requirements, UL 62368-1, fulfill the requirements of 9.3 (Electrical Protection), 10 (Servicing Protection), 11.1, 11.3 – 11.10 (Enclosure), 12 (Electric Shock), 13 (Corrosion Protection), 14 (Field Wiring Connections, General), 15 (Cord Connected Products), 18 (Grounding), 19 (Internal Wiring, General), 20 (Wiring Methods), 22.1 (Mounting of Components), 22.2 (Insulating Materials), 22.3 (Current-Carrying Parts), 24 (Printed-Wiring Boards), 25 (Transformers and Coils), 27 (Across-the-Line Components), 30 (Switches), and 33 (Spacings, General).

## 9.2 Product assembly

9.2.1 A product shall use materials that have been determined to comply with the requirements for the particular use, as indicated by the performance requirements of this standard.

9.2.2 The product shall be factory-built as a complete assembly and shall include all the components necessary for its intended function when installed and used as intended. The product may be shipped from the factory as two or more major subassemblies. See 9.2.3.

9.2.3 If the product is not assembled by the manufacturer as a complete unit, it shall be arranged in major subassemblies. Each subassembly shall be capable of being incorporated into a complete assembly without requiring alteration, cutting, drilling, threading, welding, or similar tasks by the installer. Two or more subassemblies, which must bear a definite relationship to each other for the correct installation or operation of the product, shall be arranged and constructed to permit them to be incorporated into the complete assembly only in the correct relationship with each other as indicated in the product installation instructions without the need for alteration or alignment, or such subassemblies shall be assembled, tested, and shipped from the factory as one unit.

## 9.3 Electrical protection

9.3.1 Louvers and other openings in the enclosure shall be constructed and located to reduce the risk of unintentional contact with uninsulated high-voltage live parts or film-coated wire. In determining compliance with this requirement, parts such as covers, panels, and grilles used as part of the enclosure are to be removed unless tools are required for their removal or an interlock is provided. See also Servicing Protection, Section 10.

9.3.2 Uninsulated high-voltage live parts shall be located, guarded, or enclosed as indicated in 11.3.1.1 – 11.3.1.3.

9.3.3 Knockouts or openings in an alarm sounding device housing for the connection of circuits shall be in the mounting surface only.

9.3.4 If provision is made for testing the condition of a product, such as a power supply, the means provided shall not result in a risk of electric shock, fire, or injury to persons.

# 10 Servicing Protection

## 10.1 General

10.1.1 Uninsulated live parts of high-voltage circuits, hazardous moving parts, and sharp corners and projections within the enclosure, shall be formed, located, guarded, or enclosed so as to reduce the risk of unintentional contact by persons performing service functions that may be performed while the equipment is energized.

10.1.2 During the examination of a product in connection with the requirements in 10.1.1, a part of the outer enclosure that may be removed without the use of tools, or part of the outer enclosure that may be removed by the user to allow access for making routine operating adjustments, shall be disregarded; and it shall be assumed that the removable part in question does not afford protection against the risk of electric shock.

10.1.3 The following are not considered to be uninsulated live parts:

a) Coils of relays and solenoids, and transformer windings, if the coils and windings are provided with insulating overwraps rated for the potentials encountered;

b) Terminals and splices with insulation rated for the potential encountered; and

c) Insulated wire.

## 10.2 Trained service personnel

10.2.1 When the linear distance from a component requiring servicing or an operating switch and any uninsulated current-carrying parts of high-voltage circuits is less than 6 inches (152 mm), then protection by properly applied insulating tape, barriers, or equivalent, shall be provided.

*Exception: Not applicable for products complying with the Electric Shock Current Test, Section 51.*

10.2.2 Insulating barriers, or equivalent required by 10.2.1 shall be permanently and prominently marked with the cautionary marking “CAUTION – High Voltage” or equivalent.

10.2.3 In lieu of the minimum 6 inches (152 mm) requirement only for serviceable components, the product shall comply with one of the following:

a) An interlock shall be provided on the cover to de-energize all live parts in the enclosure; or

b) The following permanent and prominent marking shall be provided on the cover front: "CAUTION – De-Energize Unit Prior To Servicing."

## 10.3 Antenna terminal discharge assembly

10.3.1 Each terminal provided for the connection of an external antenna shall be conductively connected to the supply circuit grounded conductor. The conductive connection shall have a maximum resistance of 5.2 MΩ, a minimum wattage rating of 1/2 W, and shall be effective with the power switch in either the on or off position.

*Exception No. 1: The conductive connection need not be provided when:*

*a) Such a connection is established in the event of electrical breakdown of the antenna isolating means;*

*b) The breakdown does not result in a risk of electric shock; and*

*c) In a construction using an isolating power transformer, the resistance of the conductive connection between the supply circuit and chassis does not exceed 5.2 MΩ.*

*Exception No. 2: A component comprised of a capacitor with a built-in shunt resistor that complies with the requirements for antenna-isolating capacitors is to be rated a minimum of 1/4 W.*

*Exception No. 3: The requirement is not applicable for antennas that are completely insulated with no accessibility to the risk of electric shock.*

10.3.2 The maximum value of 5.2 MΩ specified in 10.3.1 is to include the maximum tolerance of the resistor value used; that is, a resistor rated 4.2 MΩ with 20 % tolerance or a resistor rated 4.7 MΩ with a 10 % tolerance.

# 11 Enclosures

## 11.1 General

11.1.1 All electrical parts of a product shall be enclosed to provide protection of internal components and prevent contact with uninsulated live parts.

11.1.2 Operating parts, such as gear mechanisms, light-duty relays, and similar devices, shall be enclosed to protect against malfunction due to dust or other material which may impair their intended operation.

11.1.3 The enclosure of a product shall have the strength and rigidity to resist total or partial collapse and the attendant reduction of spacings, loosening or displacement of parts, or other defects. See the Mechanical Strength Tests for Enclosures, Section 66.

11.1.4 Internal parts such as the printed wiring board, power supply, etc., shall be provided with a means for mounting.

11.1.5 An enclosure containing other than power-limited circuits shall be constructed to reduce the possibility of emission of flame, flaming or glowing particles, or flaming drops. See the Abnormal Operation Test, Section 58, and/or the Ignition Test Through Bottom-Panel Openings per the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

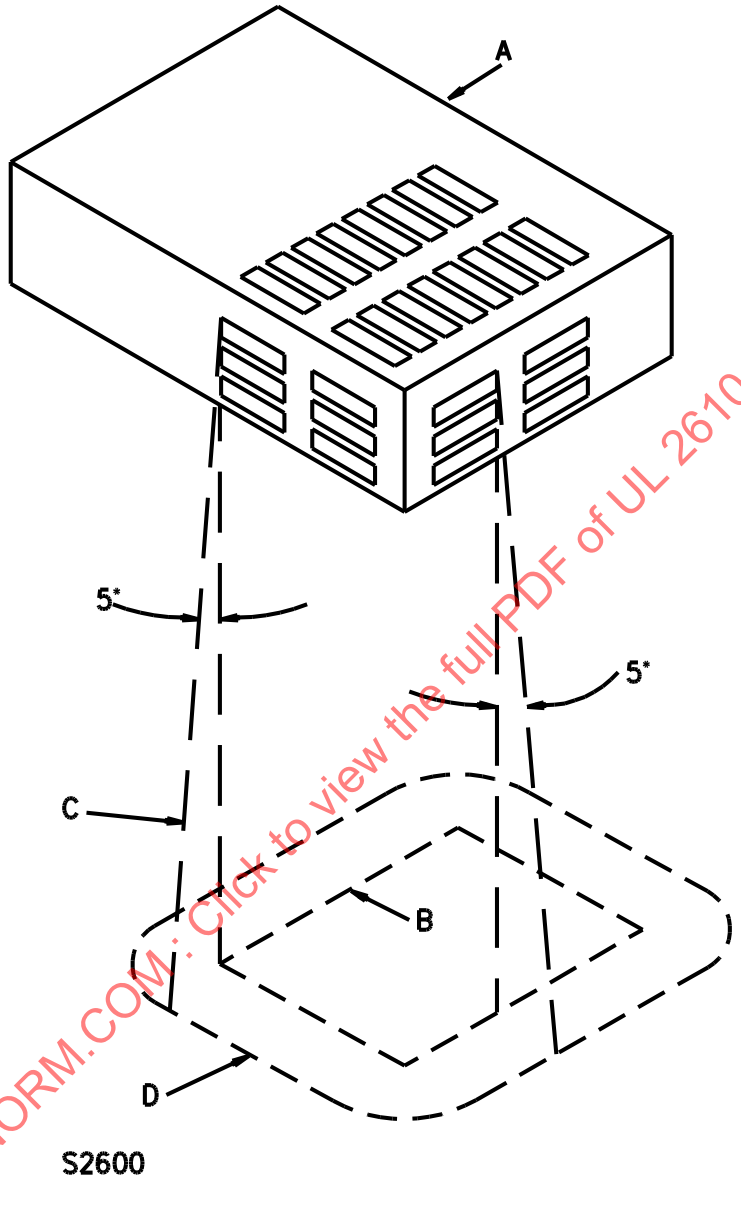
11.1.6 The requirement in 11.1.5 necessitates either a nonflammable bottom in accordance with the requirements in 11.3.4.2, or a protective barrier as illustrated in Figure 11.1 under all areas containing combustible materials.

*Exception: Openings not larger than 1/16 square inch (40.3 mm$^2$) may be provided for the bottom of the enclosure under areas containing only materials rated V-1 or less flammable. See 11.3.4.3.*

11.1.7 A construction employing individual barriers under components, groups of components or assemblies, as illustrated in Figure 11.1, is considered to comply with the requirement in 11.1.5.

**Figure 11.1**

**Enclosure Bottom**






A – The entire component under which an enclosure (flat or dished with or without a lip or other raised edge) of noncombustible material is to be provided. The sketch is of an enclosed component with ventilation openings showing that the enclosure is required only for those openings through which flaming parts are to be emitted. When the component or assembly does not have its own noncombustible enclosure, the area to be protected is the entire area occupied by the component or assembly.

B – Projection of the outline of the area of A that requires a bottom enclosure vertically downward onto the horizontal plane of the lowest point on the outer edge D of the enclosure.

C – Inclined line that traces out an area D on the horizontal plane of the enclosure. Moving around the perimeter of the area B that requires a bottom enclosure, this line projects at a 5° angle from the line extending vertically at every point around the perimeter of A and is oriented to trace out the largest area; except that the angle shall be less than 5° when the enclosure bottom contacts a vertical enclosure or side panel, or when the horizontal extension of the enclosure B to D exceeds 6 inches (152 mm).

D – Minimum outline of the enclosure, except that the extension B to D is not required to exceed 6 inches (152 mm), flat or dished with or without a tip or other raised edge. The bottom shall either be flat or formed in any manner when every point of area D is at or below the lowest point on the outer edge of the enclosure.

## 11.2 Doors and covers

11.2.1 An enclosure cover shall be hinged, sliding, pivoted or similarly attached so it cannot be removed if it:

a) Gives access to fuses or any other overcurrent protective device, the intended functioning of which requires renewal or resetting; or

b) Is necessary to open the cover in connection with the intended operation of the unit.

*Exception No. 1: If the cover position is supervised by a tamper contact that is connected in the closed protective circuit, an enclosure need not comply with the requirements of this paragraph. See also 41.10.*

*Exception No. 2: These requirements do not apply to a product located at a monitoring station.*

11.2.2 Fasteners requiring the use of a tool or key shall be used for the assembly of all enclosures if access is not required for operation of the product.

*Exception: This requirement does not apply to a product located at a monitoring station.*

11.2.3 The cover of an enclosure shall be provided with a supervisory contact, connected in the closed protective wiring circuit, if it gives access to any relays, terminals, controls, or related components that might be subject to tampering without causing an alarm or trouble signal. See also 41.10.

*Exception: An enclosure located inside of a completely protected safe or vault does not require tamper protection.*

## 11.3 Enclosure openings

### 11.3.1 General

11.3.1.1 Openings in the enclosure shall be constructed and of such size so that direct entry of foreign objects is prevented. See also 11.3.2.1. See Figure 11.4 for examples of acceptable top cover constructions that are deemed to prevent direct entry. See also Figure 11.5 for acceptable side opening constructions.

11.3.1.2 An opening in an electrical enclosure that does not permit entrance of a 1 inch (25.4 mm) diameter rod shall be sized and arranged so that a probe, as illustrated in Figure 11.2, cannot be made to contact any uninsulated live part (other than low-voltage) when inserted through the opening in a straight or articulated position. The probe illustrated shall be applied to any depth that the opening will permit and rotated or angled before, during, or after insertion through the opening to any position that is required in order to examine the enclosure.

11.3.1.3 An opening that permits entrance of a 1 inch (25.4 mm) diameter rod is acceptable under the conditions described and illustrated in Figure 11.3.

**Figure 11.2**

**Accessibility Probe with Web Stop**

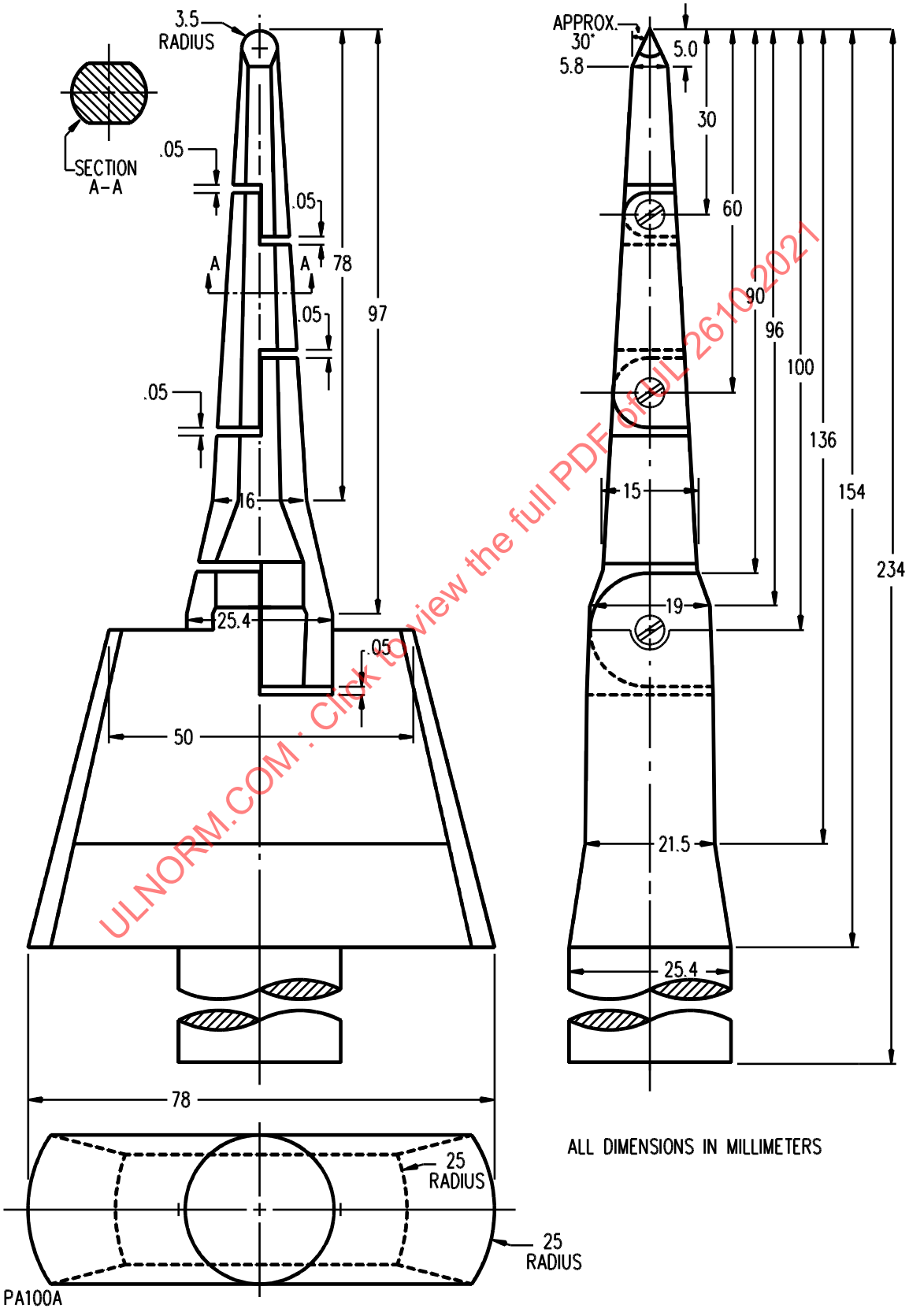
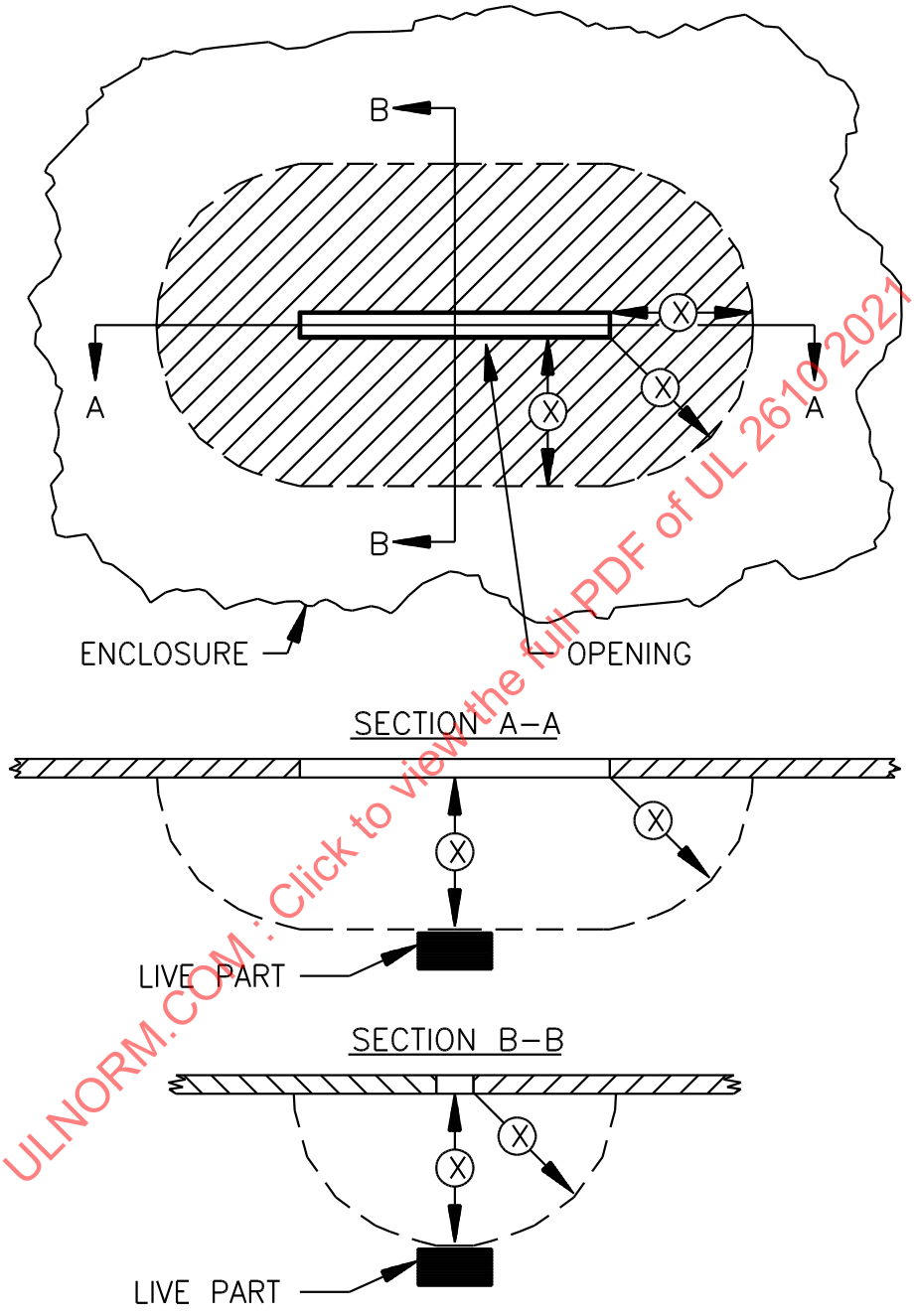


**Figure 11.3**

**Opening in Enclosure**




EC100A

NOTE – The opening may be used if, within the enclosure, there is no uninsulated live part or film coated wire:

a) Less than X inches (mm) from the perimeter of the opening, as well as;

b) Within the volume generated by projecting the perimeter X inches (mm) normal to its plane.

X equals five times the diameter of the largest diameter rod that can be inserted through the opening, but not less than 6-1/16 inches (154 mm).

11.3.1.4 Openings are acceptable, without limitation of the size or number of openings, in areas containing only PVC, TFE, CTFE, FEP, and neoprene insulated wire or cable, in areas containing plugs and receptacles, and in areas underneath impedance protected or thermally protected motors.

11.3.1.5 Openings in the enclosure shall not give access to relays, terminals, controls, or related components that might be subject to tampering by hand or with tools without causing an alarm or trouble signal.

11.3.1.6 An enclosure intended for recessed mounting and whose front panel is to be flush with the surface of the wall shall have no openings that vent into concealed spaces of a building structure, such as into hollow spaces in the wall, when the product is mounted as intended.

*Exception: Not applicable for products supplied solely from power-limited sources and controlling only power-limited loads.*

11.3.1.7 The requirement in 11.3.1.6 does not apply to an opening for a mounting screw or nail or for a manufacturing operation (such as paint drainage) when:

a) An opening for non-mounting purposes does not have a dimension greater than 17/64 inch (6.75 mm) or an area greater than 0.055 $ft^2$ (35.5 $mm^2$); and

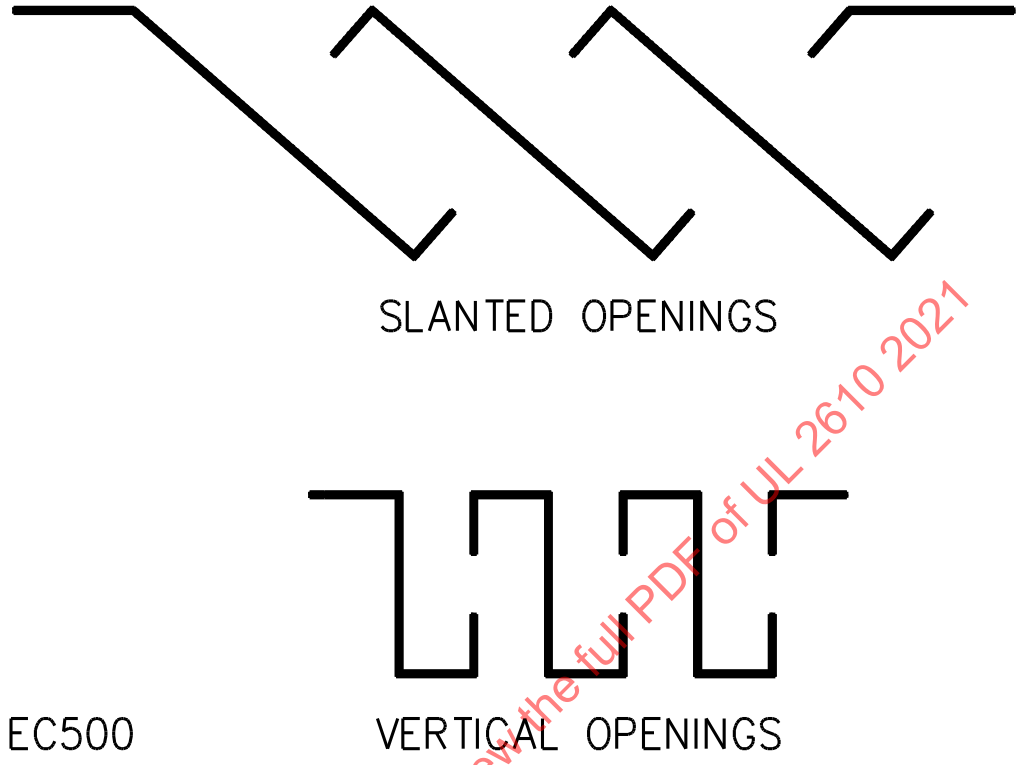
b) An opening for mounting does not have a dimension greater than 0.75 inch (19.05 mm) or an area greater than 0.7 $inch^2$ (430 $mm^2$) and there are no more holes than are needed to mount the product.

### 11.3.2 Enclosure top openings

11.3.2.1 Openings directly over uninsulated high voltage live parts shall not exceed 0.20 inch (5.0 mm) in any dimension unless the configuration is such that a vertically falling object cannot fall into the unit and contact an uninsulated live part. For examples complying with the intent of this requirement, see Figure 11.4 for top cover designs.

**Figure 11.4**

**Cross Sections of Top Cover Designs**






### 11.3.3 Enclosure side openings

11.3.3.1 An opening in the side of the enclosure shall:

a) Not exceed 0.20 inch (5.0 mm) in any dimension;

b) Be provided with louvers shaped to deflect an external falling object outward (see Figure 11.5 for examples of louver designs complying with the requirement); or

c) Be located and sized so that objects which are present cannot drop into the unit and fall (with no horizontal velocity) onto uninsulated live parts involving a risk of fire, electric shock, or electrical-energy/high-current levels, or parts involving injury to persons (see Figure 11.6).