UL 294

STANDARD FOR SAFETY

Access Control System Units

UL Standard for Safety for Access Control System Units, UL 294

Eighth Edition, Dated May 24, 2023

Summary of Topics

This new edition of ANSI/UL 294 dated May 24, 2023, includes updates, clarifications, and revisions throughout including the following:

- ***Power over communication cable equipment updates***
- ***Remote Access requirements***
- ***Software/Firmware Upgrades***
- ***Egress Control Systems Requirements***
- ***Key Management System Requirements***
- ***Overload and Endurance Test (power supply) updates***
- ***Destructive Attack Test updates***

The new and revised requirements are substantially in accordance with Proposal(s) on this subject dated July 29, 2022 and February 17, 2023.

No Text on This Page

MAY 24, 2023

ANSI/UL 294-2023

UL 294

Standard for Access Control System Units

First Edition – May, 1974
Second Edition – September, 1980
Third Edition – January, 1987
Fourth Edition – June, 1994
Fifth Edition – January, 1999
Sixth Edition – May, 2013
Seventh Edition – January, 2018

Eighth Edition

May 24, 2023

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

The most recent designation of ANSI/UL 294 as an American National Standard (ANSI) occurred on May 24, 2023. 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 ULSE at any time. Proposals should be submitted via a Proposal Request in ULSE's Collaborative Standards Development System (CSDS) at https://csds.ul.com.

No Text on This Page

CONTENTS

INTRODUCTION

1 Scope 9
2 General Information 9
3 Components 10
4 Units of Measurement 11
5 Referenced Publications 11
6 Glossary 13
7 Performance Level Definitions For Access Control 18
8 Information Required for Assessment 19
9 Version Number 19

CONSTRUCTION

ASSEMBLY

10 General 20
10.1 Specific product requirements 20
10.2 Product assembly 20
10.3 Electrical protection 21
11 Protection of Service Personnel 24
12 Enclosure 24
12.1 General 24
12.2 Doors and covers 26
12.3 Enclosure openings – general 26
12.4 Enclosure top openings 26
12.5 Enclosure side openings 27
12.6 Enclosure bottom openings 30
12.7 Screens and expanded metal 31
12.8 Cast metal 31
12.9 Sheet metal 32
12.10 Product enclosure mounting 35
12.11 Polymeric materials 35
13 Electric Shock 35
14 Corrosion Protection 36

FIELD WIRING CONNECTIONS

15 General 36
16 Cord Connected Products 37
17 Permanently Connected Products 37
17.1 General 37
17.2 Power Limited/Class 2 or 3 circuits 38
17.3 Field-wiring terminals 39
17.4 Qualified application 40
17.5 Field wiring leads 41
17.6 Polarity identification 42
18 Grounding 42

INTERNAL WIRING

19 General 43

20 Wiring Methods 43
21 Separation of Circuits 44
22 Bonding for Grounding 45

COMPONENTS, ELECTRICAL

23 Mounting of Components 47
24 Insulating Materials 48
25 Fuseholders and Current-Carrying Parts 49
26 Overcurrent Protection 49
27 Semiconductors 49
28 Switches 49
29 Transformers and Coils 49
30 Rechargeable Storage-Type Batteries Used as a Secondary Power Source 50
31 Nonrechargeable (Primary) Dry-Cell Batteries 50
32 Lithium Batteries 51

SPACINGS

33 General 51
34 Components 53

PERFORMANCE – ALL UNITS

35 General 53
35.1 General information 53
35.2 Single point locking devices 54
35.3 Test units and data 55
35.4 Test samples and miscellaneous data 55
35.5 Test voltages 56
35.6 Essential computer equipment 56
35.7 Power over communications cable equipment 57
35.8 Remote access 59
35.9 Egress control systems 65
35.10 Key management systems 65
36 Normal Operation Test 67
37 Electronic Authentication 67
38 Input Measurement Test 68
39 Output Measurement Test 68
40 Power-Limited/Class 2 and Class 3 Circuits Test 69
40.1 General 69
40.2 Maximum voltage 71
40.3 Maximum current 71
40.4 VA_{max} (not inherently limited circuits only) 72
41 Electrical Supervision Test 72
41.1 General 72
41.2 Power interruption 72
42 Standby Power 72
43 Undervoltage Operation Test 73
44 Overvoltage Operation Test 73
45 Variable Ambient Test 73
46 Humidity Test 73
47 Leakage Current Test for Cord-Connected Products 74
48 Electric Shock Current Test 76
49 Overload Test 80

49.1 General....80
49.2 Separately energized circuits....80
49.3 Power supplies....80
50 Endurance Test....81
50.1 General....81
50.2 Separately energized circuits....81
50.3 Power supplies....82
51 Jarring Test....82
52 Dielectric Voltage-Withstand Test....83
53 Temperature Test....85
54 Abnormal Operation Test....88
55 Electrical Transient Tests....88
55.1 General....88
55.2 Supply line (ring wave surge voltage) transients....89
55.3 Internally induced transients....89
55.4 Input/output (low-voltage) field-wiring transients....89
56 AC Induction Test....96
57 Communication Circuits....97
58 Polymeric Materials Test....97
59 Battery Replacement Test....97
60 Drop Test....97
61 Strain Relief Test....98
61.1 General....98
61.2 Field-wiring leads....98
62 Tests for Ignition Through Bottom-Panel Openings....98
62.1 General....98
62.2 Hot, flaming oil....98
62.3 Molten PVC and copper....99
63 Mechanical Strength Tests for Enclosures....99
63.1 Constant-force test....99
63.2 Impact test....100
64 Special Terminal Assemblies Tests....100
64.1 General....100
64.2 Disconnection and reconnection....100
64.3 Mechanical secureness....101
64.4 Flexing test....101
64.5 Millivolt drop test....101
64.6 Temperature test....101
65 Destructive Attack Test....101
66 Destructive Attack Alarm Test....102
67 Access Control Line Security....103
67.1 General....103
67.2 Access Control Line Security Level II – Standard line security....103
67.3 Access Control Line Security Level III – Encrypted line security with 128 bit encryption....104
67.4 Access Control Line Security Level IV – Encrypted line security with 256 bit encryption....104
68 Biometric Test....104
69 Controlled And Delayed Egress Equipment And Systems Operation....105
69.1 General Requirements....105
69.2 Delayed egress requirements....106
69.3 Controlled egress requirements....106

MANUFACTURING AND PRODUCTION LINE TESTS

70 Production Line Dielectric Voltage-Withstand Test For High-Voltage Products....107

71 Production Line Grounding Continuity Test 107

MARKINGS

72 Details 108
73 Marking Permanency Tests 110

OUTDOOR USE EQUIPMENT

ASSEMBLY

74 General 110
75 Construction 111
75.1 General 111
75.2 Corrosion protection 111
76 Field-Wiring Connections 113
77 Internal Wiring 113
78 Components, Electrical Insulating Material 114

PERFORMANCE

79 Rain Test 114
80 Dust Test 118
81 Variable Ambient Test 118
82 Metallic Coating Thickness Test 118
83 Corrosion Tests 120
83.1 General 120
83.2 Salt spray (fog) 120
83.3 Moist hydrogen sulfide (H_2) – air mixture 121
83.4 Moist carbon dioxide (CO_2) – sulfur dioxide (SO_2) – air mixture 121
83.5 Alternate corrosion test (21-day) 121
84 Ultraviolet Light and Water Exposure Test 122
85 Accelerated Aging Tests for Gaskets, Sealing Compounds, and Adhesives 122
85.1 General 122
85.2 Gasket low temperature test – Outdoor use 124

MARKINGS

86 Details 125

ACCESSORY EQUIPMENT

87 General 125
88 Construction 125
89 Performance (Installation) Test 126
90 Markings 126

INSTRUCTIONS

91 Installation and Operating Instructions 126

ANNEX A (informative) – STANDARDS FOR COMPONENTS

ANNEX B (informative) – POWER OVER ETHERNET (PoE) REFERENCE

B1 Definitions 133
B2 Ratings (Per Pair) 133
B.3 Reference Publications 133

No Text on This Page

INTRODUCTION

1 Scope

1.1 These requirements apply to the construction, performance, and operation of physical access control equipment and/or systems intended to regulate or control:

a) Entry into and/or exit from a controlled area, protected area or a restricted area or

b) Access to or the use of a device(s) by electrical, electronic or mechanical means.

1.2 The extent of control of entry/exit may include the reporting and recording of related activity. The accuracy of the logged data is not evaluated by this standard.

1.3 This standard defines the minimum requirements as they apply to the construction, performance and operation of such systems, equipment and/or computer equipment as well as tiered characteristics to meet four levels of security performance with Level I (lowest level security equipment) to Level IV (highest level security equipment).

1.4 Where an access control equipment and/or system incorporates the features and functions of a burglar alarm control unit, the requirements of the Standard for Proprietary Burglar Alarm Units and Systems, UL 1076, or the applicable section of the Standard for Commercial Premises Security Alarm Units and Systems, UL 2610, shall also apply.

1.5 These requirements apply to computer equipment that, when used in conjunction with the main control unit, is necessary to support the operation (granting (authorized) or denying (unauthorized) access) of the access control system. This Standard does not apply to supplementary computer equipment that is not necessary for operation of the access control system if electrical transients or single opens, earth ground faults or wire-to-wire shorts on the circuit connection from the computer to the access control system does not inhibit intended operation or provide unauthorized entry.

2 General Information

2.1 For equipment utilizing power over communications cables, refer to 35.7, Power over communications cable equipment. Compliance with IEEE 802.3 (at or af) specifications shall not be verified as part of these requirements.

2.2 Biometric equipment parameters such as False Acceptance Rate (FAR), False Rejection Rates (FRR), Failure to Enroll, Failure to Acquire, and other biometric quality parameters, are not specifically evaluated as part of this standard. See Section 68, Biometric Test.

2.3 Access control systems that include duress signaling features are additionally evaluated per UL 636, or the applicable section of UL 2610.

2.4 Products intended for use in air-handling spaces in Accordance with Section 300.22, (C) of 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.

2.5 Products that utilize input, output and/or control devices that are not interconnected by a solid medium, such as cable, optical fiber, or the like, but provide signaling by means of low power radio frequency (RF) defined by the Code of Federal Regulations (CFR), Title 47, Part 15, shall comply with the Short-Range Radio Frequency (RF) Tests in UL 2610, as applicable. The following tests are not considered necessary for access control products:

a) Clash Error;

b) Interference Protection;

c) Tamper Protection; and

d) Time to Report Alarm.

Exception No. 1: Wireless access control credentials (i.e. cards, tokens, electronic devices) are not subject to the RF requirements noted.

Exception No. 2: Egress control systems (i.e. Infant Protection/Patient Wandering systems; see 35.9) are subject to all RF tests noted in UL 2610 (Short-Range Radio Frequency (RF) Tests). When the tag or credential of an egress control system is an active element of the intended two-way RF transmission functionality, the tag/credential is also subject to the RF tests noted above as applicable.

2.6 Unless otherwise specified, the fundamental compliance criteria of this Standard indicates that the access control system and its components shall not inhibit intended operation, or provide unauthorized entry, when subject to the tests and requirements documented within.

2.7 Electromechanical or electromagnetic door locking devices are typically evaluated in accordance with UL 1034.

2.8 Systems and components may also be utilized in accordance with NFPA 101, International Building Code and the like.

3 Components

3.1 Except as indicated in 3.2, a component of a product covered by this standard shall comply with the requirements for that component. See Annex A for a list of Standards covering components generally used in the products covered by this standard.

3.2 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.

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

3.4 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.

3.5 Compliance of laser products with the Code of Federal Regulations (CFR), Title 21, Part 1040, shall be determined by:

a) Determining the Class of the laser product and the Class of the radiation emitted by the laser product (as defined in the CFR) from the manufacturer's Center for Devices and Radiological Health (CDRH) product report;

b) Verifying that the manufacturer’s markings and labels having the information specified in the CFR are affixed on the laser product (as defined in the CFR);

c) Determining that the corresponding construction features, such as protective housing, interlocks, and similar features, are provided in accordance with the CFR;

d) Determining that the resulting construction complies with the construction requirements of this standard; and

e) Verifying that the manufacturer's safety instructions required by the CFR are provided with the laser product (as defined in the CFR).

4 Units of Measurement

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

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

5 Referenced Publications

5.1 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.

5.2 The following publications are referenced in this Standard:

ANSI C80.1, *Specifications for Zinc-Coated Rigid Steel Conduit*

ANSI S12.31, *Precision Methods for the Determination of Sound Power Levels of Broad Band Noise Sources in Reverberation Rooms*

ANSI S12.32, *Precision Methods for the Determination of Sound Power Levels of Discrete Frequency and Narrow Band Noise Sources in Reverberation Rooms*

ASTM A653/A653M, *Specification for Steel Sheet, Zinc-Coated (Galvanized) or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process*

ASTM A90/A90M, *Standard Test Method for Weight (Mass) of Coating on Iron and Steel Articles with Zinc or Zinc-Alloy Coatings*

ASTM B117, *Standard Practice for Operating Salt Spray (Fog) Apparatus*

ASTM D396, *Standard Specification for Fuel Oils*

ASTM D412, *Standard Test Methods for Vulcanized Rubber and Thermoplastic Rubbers and Thermoplastic Elastomers – Tension*

ASTM E230/E230M, *Standard Specification and Temperature-Electromotive Force (emf) Tables for Standardized Thermocouples*

47 CFR Part 15, *Radio Frequency Devices*

FIPS 46-3, *Federal Information Processing Standard, Data Encryption Standard*

FIPS 140-2, *Security Requirements for Cryptographic Modules*

FIPS 180-4, *Secure Hash Standard (SHS)*

FIPS 185, *Escrowed Encryption Standard*

FIPS 186-4, *Digital Signature Standard (DSS)*

FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*

FIPS 197, *Federal Information Processing Standard, Advanced Encryption Standard*

IEEE 802.3, *Standard for Ethernet*

IEC 61000-4-5, *Surge Tests per Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEEE 1394, *Standard for a High-Performance Serial Bus*

IEEE C62.41, *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*

MIL-STD-338, *Cleaning and Treatment of Aluminum Parts Prior to Painting*

MIL-STD-750F, *Test Methods for Semiconductor Devices*

MIL-STD-883H, *Department of Defense Test Method Standard: Microcircuits*

NFPA 70, *National Electrical Code*

NFPA 101, *Life Safety Code*

NIST SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*

NIST SP 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

TIA-568-C.2, *Balanced Twisted-Pair Telecommunications Cabling and Components*

UL 50, *Enclosures for Electrical Equipment, Non-Environmental Considerations*

UL 305, *Panic Hardware*

UL 310, *Electrical Quick-Connect Terminals*

UL 437, *Key Locks*

UL 486A-486B, *Wire Connectors*

UL 486E, *Equipment Wiring Terminals for Use with Aluminum and/or Copper Conductors*

UL 497A, *Secondary Protectors for Communications Circuits*

UL 497B, *Protectors for Data Communications and Fire-Alarm Circuits*

UL 636, *Hold Up Units and Alarm Systems*

UL 746C, *Polymeric Materials – Use in Electrical Evaluations*

UL 796, *Printed Wiring Boards*

UL 827, *Central-Station Alarm Services*

UL 969, *Marking and Labeling Systems*

UL 1034, *Burglary-Resistant Electric Locking Mechanisms*

UL 1059, *Terminal Blocks*

UL 1076, *Proprietary Burglar Alarm Units and Systems*

UL 1449, *Surge Protective Devices*

UL 1481, *Power Supplies for Fire-Protective Signaling Systems*

UL 1642, *Lithium Batteries*

UL 1778, *Uninterruptible Power Systems*

UL 1863, *Communications-Circuit Accessories*

UL 1977, *Component Connectors for Use in Data, Signal, Control and Power Applications*

UL 2043, *Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces*

UL 2610, *Commercial Premises Security Alarm Units and Systems*

UL 60950-1, *Information Technology Equipment – Safety – Part 1: General Requirements*

UL 62368-1, *Audio/Video Information and Communication Technology Equipment – Part 1: Safety Requirements*

6 Glossary

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

6.2 The term "product" as used in this standard refers to all types of access control equipment or systems of equipment.

6.3 ACCESS CONTROL – A means and/or measure to regulate or control physical access control that may consist of:

a) Entry and/or exit to/from a controlled area, protected area or a restricted area; or

b) Physical access to or the use of a device(s) by electrical, electronic or mechanical means.

6.4 ACCESS CONTROL DESTRUCTIVE ATTACK LEVEL I _ An access control product intended for, but not limited to, a controlled area that is not required to meet the destructive Attack Test.

6.5 ACCESS CONTROL DESTRUCTIVE ATTACK LEVEL II – An access control product intended for, but not limited to, a protected area that can withstand the destructive Attack Test for 2 minutes.

6.6 ACCESS CONTROL DESTRUCTIVE ATTACK LEVEL III – An access control product intended for, but not limited to, a restricted area that can withstand the destructive Attack Test for 5 minutes, or 2 minutes if an alarm is activated during the test.

6.7 ACCESS CONTROL DESTRUCTIVE ATTACK LEVEL IV – An access control product intended for, but not limited to, a restricted area that can withstand the destructive attack test for 5 minutes, generate an alarm signal in 2 minutes and the alarm cannot be silenced until acknowledged by the operator for 2 minutes.

6.8 ACCESS CONTROL ENDURANCE LEVEL I – An access control product shall operate as intended at rated voltage and current for 1,000 cycles of intended operation.

6.9 ACCESS CONTROL ENDURANCE LEVEL II – An access control product shall operate as intended at rated voltage and current for 25,000 cycles of intended operation.

6.10 ACCESS CONTROL ENDURANCE LEVEL III – An access control product shall operate as intended at rated voltage and current for 50,000 cycles of intended operation.

6.11 ACCESS CONTROL ENDURANCE LEVEL IV – An access control product shall operate as intended at rated voltage and current for 100,000 cycles of intended operation.

6.12 ACCESS CONTROL LINE SECURITY – Equipment incorporates refinement in electric apparatus and circuit arrangement to guard against an attempt to compromise the connecting line or communication channel between two access control products or equipment.

6.13 ACCESS CONTROL LINE SECURITY LEVEL I – An access control product with no communication line security.

6.14 ACCESS CONTROL LINE SECURITY LEVEL II – An access control product provided with standard communication line security. See 67.2.

6.15 ACCESS CONTROL LINE SECURITY LEVEL III – An access control product provided with 128-bit encryption. See 67.3.

6.16 ACCESS CONTROL LINE SECURITY LEVEL IV – An access control product provided with 256 bit encryption. See 67.4.

6.17 ACCESS CONTROL STANDBY POWER LEVEL I – An access control product designed with no secondary power source.

6.18 ACCESS CONTROL STANDBY POWER LEVEL II – An access control product that operates as intended with a loss of primary power for 30 minutes while the product is operated every minute.

6.19 ACCESS CONTROL STANDBY POWER LEVEL III - An access control product that operates as intended with a loss of primary power for 2 hours while the product is operated every minute.

6.20 ACCESS CONTROL STANDBY POWER LEVEL IV – An access control product that operates as intended, and with a loss of primary power for 4 hours while the product is operated every minute.

6.21 ACCESS CONTROL SYSTEM – A collection of means, measures and specific practices that when combined, form or compose a systematic approach, which enables an authority to control access to areas and resources in a given physical facility. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

6.22 ACCESS CONTROL UNIT – A part of the access control system that interfaces with readers, locking devices and sensing devices, making a decision to grant or deny access.

6.23 ACCESS CONTROL UNIT ACCESSORY – Any device or component of an access control system other than the access control unit that is employed to assure intended operation of the system. Examples of access control unit accessories include: readers, keypads, request-to-exit devices, input/output interfaces, and the like.

6.24 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.)

6.25 ALARM – A condition requiring human assessment or intervention.

6.26 ALARM SIGNAL – A transmission of an alarm condition or alarm report.

6.27 BIOMETRIC(S) – Any measurable, unique physiological characteristic or personal trait that is used as a credential to recognize and verify the identity of an individual. (e.g. fingerprint, hand or face geometry, retinal/eye, face, voice, signature or keyboarding dynamics).

6.28 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 alternating current (AC), 42.4 volts direct current (DC) or AC peak.

c) Power Limited / Class 2/3 Circuit – A circuit wherein the power is limited as specified in Table 40.1 and Table 40.2.

d) Power over Communications Cable – A limited energy circuit that meets the requirements of 35.7.

e) Risk of Electric Shock – A risk of electric shock is determined to exist within a circuit unless that circuit meets one of the following criteria (1 and 2, or 3):

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; or

3) A limited energy power over communications circuit that meets the requirements of 35.7, Power over communications cable equipment.

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 35.7, Power over communications cable equipment, for equipment utilizing power over communications cables.

6.29 CONTROLLED AREA – A room, office, building, facility, premises, or grounds to which access is monitored, limited, or controlled.

6.30 CONTROLLED EGRESS EQUIPMENT AND SYSTEMS – A door-latching assembly incorporating a device such as an electric or electromagnetic locking mechanism that controls the releases latch on an egress door.

6.31 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.

6.32 CREDENTIAL – Any token, card, memorized or stored information, biometric image, or electronic means used to identify an individual to an access control system in order to verify user access rights.

6.33 CRITICAL COMPONENT – A critical component is one whose malfunctioning will impair the normal operation of the product, grants unauthorized access or creates a risk of fire or electrical shock.

6.34 DELAYED EGRESS EQUIPMENT AND SYSTEMS – A door-latching assembly incorporating a time-delay feature that controls the release latch on an egress door upon the application of a force in the direction of egress travel.

6.35 EGRESS CONTROL SYSTEM - A system that is used to control the unauthorized egress of patients and/or infants from secured areas within a hospital or other healthcare facility. See 35.9.

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

6.37 EQUIPMENT – Any part of an electronic access control system, such as access control units, readers, reader interface modules, access point actuators, access point sensors, keypads, and the like.

6.38 ESSENTIAL COMPUTER EQUIPMENT – Computer equipment connected to the access control system either on or off premises that is relied upon, or can perform, access control operations.

6.39 ETHERNET CABLING – A structured cabling system using 4 pair unshielded or shielded twisted pair cable, meeting Category 5e performance or higher and conforming to 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.

6.40 FAIL SAFE – A condition under which the product ceases to operate in such a way as to automatically allow access or egress.

6.41 FAIL SECURE – A condition under which the product ceases to operate in such a way as to not allow unauthorized access or unauthorized egress.

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

6.43 HARDWARE – Physical equipment that constitutes the components of an access control system.

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

6.45 KEY MANAGEMENT SYSTEM – Key management systems provide a means of regulating or controlling keys by electrical, electronic and/or mechanical means, and allow authorized users access to keys upon verification of appropriate credentials. See 35.10.

6.46 LINE-VOLTAGE – The voltage (commonly 115, 208, and 230 volts) at any field-connected source of supply, nominally 50 – 60 hertz (Hz).

6.47 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).

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

6.49 NORMAL STANDBY CONDITION – The ready-to-operate condition that exists prior to being operated.

6.50 POWER INJECTOR (Alternative terms – Injector or 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.

6.51 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 Annex B) and USB.

6.52 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.

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

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

6.55 PROTECTED AREA – A room, office, building, facility, premises or grounds to which access is monitored, and limited and/or controlled, whereby the authorized person of the Access Control System may grant access to non-authorized persons.

6.56 RESTRICTED AREA – A room, office, building, facility, premises, or grounds to which access is monitored, limited and strictly controlled, whereby only the administrator of the Access Control System shall issue credentials that will lead to access.

6.57 SECONDARY BATTERY – Any battery that is intended to be recharged.

6.58 SECURED AREA – Any Controlled, Protected, or Restricted Area.

6.59 SINGLE POINT LOCK – An autonomous access control solution, residing locally to the access point, where during primary operation, authorizations are stored, access decisions are made, and access is physically granted or denied within a single stand-alone product.

6.60 SOFTWARE – Instructions that are temporarily or permanently stored in the computer's memory and used to provide function and control of the computer's components.

6.61 STAND-ALONE SYSTEM/MODE – An access control solution or mode of operation which does not rely upon communication between the access control unit and/or the computer (monitoring) equipment for access control operations.

6.62 STANDBY POWER / SECONDARY POWER SOURCE – Provides power when the primary power source fails.

6.63 SYSTEM DATABASE – Information entered into the computer by authorized personnel including items such as names, security information for system users, emergency phone numbers, and graphics.

7 Performance Level Definitions For Access Control

7.1 The access control features identified in Table 7.1 shall be identified for the product or equipment by the Level specified by the manufacturer for that feature.

Table 7.1
Summarized Levels of Access Control Components

Feature	Level I	Level II	Level III	Level IV
Destructive attack	No attack test	Withstand attack test for 2 minutes	Withstand attack test for 5 minutes or generate an audible alarm in 2 minutes	Withstand attack test for 5 minutes, generate an audible alarm in 2 minutes which cannot be silenced for 2 minutes
Line security	No line security	Standard line security	Encrypted line security 128 bit	Encrypted line security 256 bit
Endurance	1000 cycles	25,000 cycles	50,000 cycles	100,000 cycles

Table 7.1 Continued on Next Page

Table 7.1 Continued

Feature	Level I	Level II	Level III	Level IV
Standby power	No secondary power source	Can maintain normal operation for a minimum of 30 minutes (see 6.18)	Can maintain normal operation for a minimum of 2 hours (see 6.19)	Can maintain normal operation for a minimum of 4 hours (see 6.20)
Single Point Locking Device with Key Locks (see 35.2.2)	No attack test on key lock	Picking, Lock Bumping and Impression tests for key locks from Attack Resistance Test Time table of UL 437	All key lock attack resistance tests from Attack Resistance Test Time table of UL 437	N/A

7.2 When a product or equipment provides standby power, the manufacturer shall specify the amount of time the product or equipment can operate normally under the specified load conditions, while on standby power. See 72.14.

7.3 The level of the access control feature may be marked on the product or equipment.

7.4 The level of access control feature shall be specified in the product or equipment documentation that is provided.

7.5 Features that exceed the levels specified for endurance and standby power shall be verified by tests and may be indicated in the product or equipment documentation. The level of access control feature shall be indicated to the highest tiered level achieved through tests.

8 Information Required for Assessment

8.1 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, Details, Sections 72 and 90.

9 Version Number

9.1 If reprogrammable, an access control product or equipment shall provide some method to identify the current version of programming logic code / software being used. Subversions that are used to identify non-critical logic changes are not required to be identified. This information shall also appear in the product installation instructions.

CONSTRUCTION

ASSEMBLY

10 General

10.1 Specific product requirements

10.1.1 Products that currently meet all the requirements of UL 60950-1 or UL 62368-1, fulfill the requirements of:

a) 10.3 (Electrical Protection);

b) Section 11 (Protection of Service Personnel);

c) 12.1, 12.3 – 12.7 (Enclosure);

d) Section 13 (Electric Shock);

e) Section 14 (Corrosion Protection);

f) Section 15 (Field Wiring Connection, General);

g) Section 16 (Cord Connected Products);

h) 17.6 (Polarity Identification);

i) Section 18 (Grounding);

j) Section 19 (Internal Wiring, General);

k) Section 22 (Bonding for Grounding);

l) Section 23 (Mounting of Components);

m) Section 24 (Insulating Materials);

n) Section 25 (Fuseholders and Current-Carrying Parts);

o) Section 28 (Switches);

p) Section 29 (Transformers and Coils); and

q) Section 33 (Spacings, General).

10.2 Product assembly

10.2.1 An access control product shall not impair the intended operation of panic hardware used in conjunction with it.

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

10.2.3 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 final assembly without requiring alteration, cutting, drilling, threading, welding, or similar tasks by the installer. Two or

more subassemblies shall be arranged and constructed to permit them to be incorporated into the complete assembly only in the intended relationship with each other, where this is necessary, without need for alteration or alignment. Otherwise, such subassemblies shall be assembled, tested, and shipped from the factory as one element.

10.3 Electrical protection

10.3.1 Louvers and other openings in the enclosure shall be constructed and located to reduce the risk of contact by persons with uninsulated high-voltage live parts. 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.

10.3.2 Uninsulated high-voltage live parts shall be located, guarded, or enclosed as indicated in 10.3.3 and 10.3.4.

10.3.3 Openings directly over uninsulated high-voltage live parts shall not exceed 0.187 inch (4.75 mm) in any dimension unless the configuration is arranged to reduce the risk of unintentional contact by persons with uninsulated high-voltage live parts. See Figure 12.2 for examples of top cover constructions which may be used.

10.3.4 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 10.1, cannot be made to contact any uninsulated live high-voltage electrical part when inserted through the opening in a straight or articulated position.

10.3.5 An opening that permits entrance of a 1-inch (25.4-mm) diameter rod may be used under the conditions described in Figure 10.2.

Figure 10.1

Articulate Probe

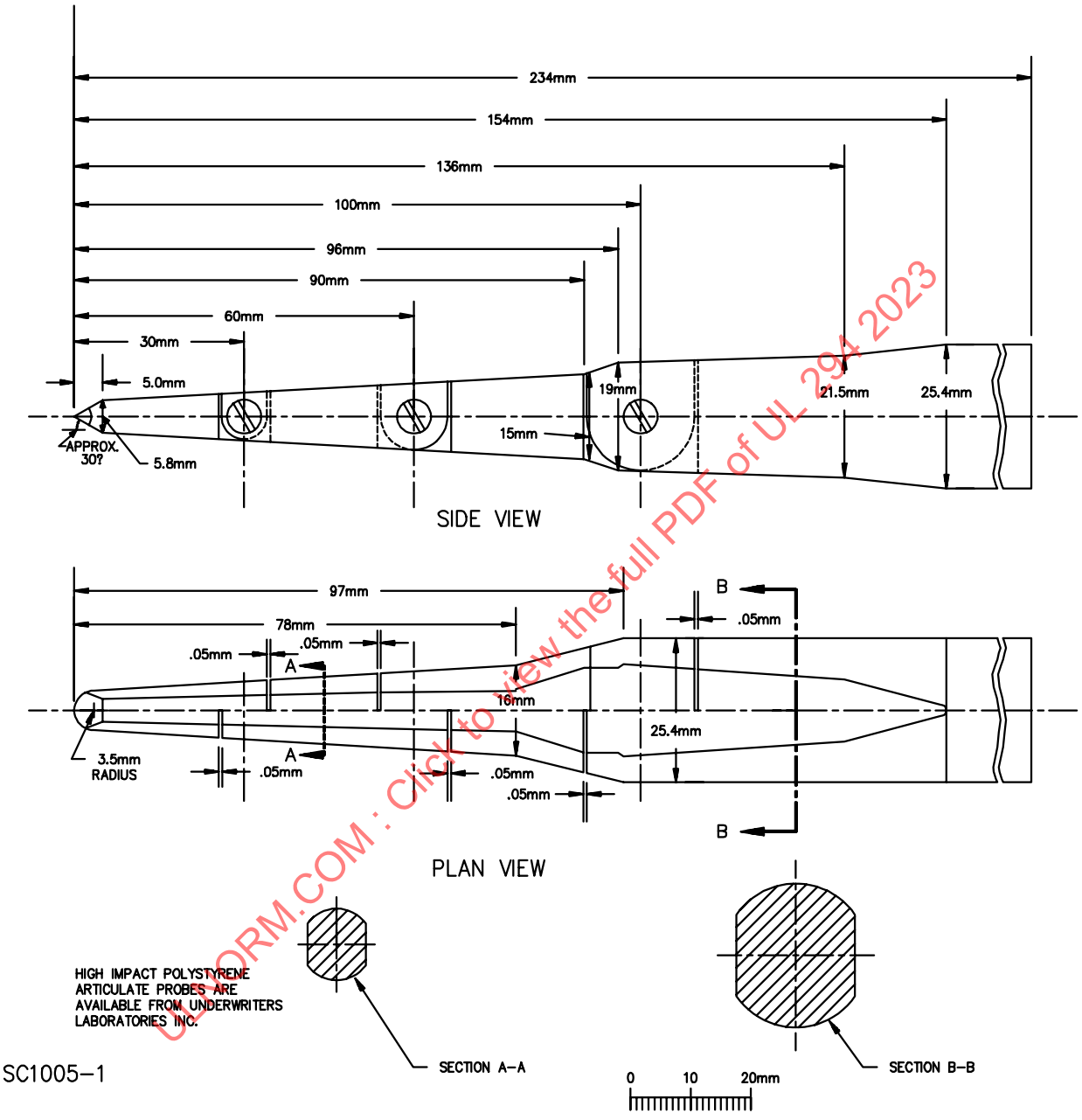
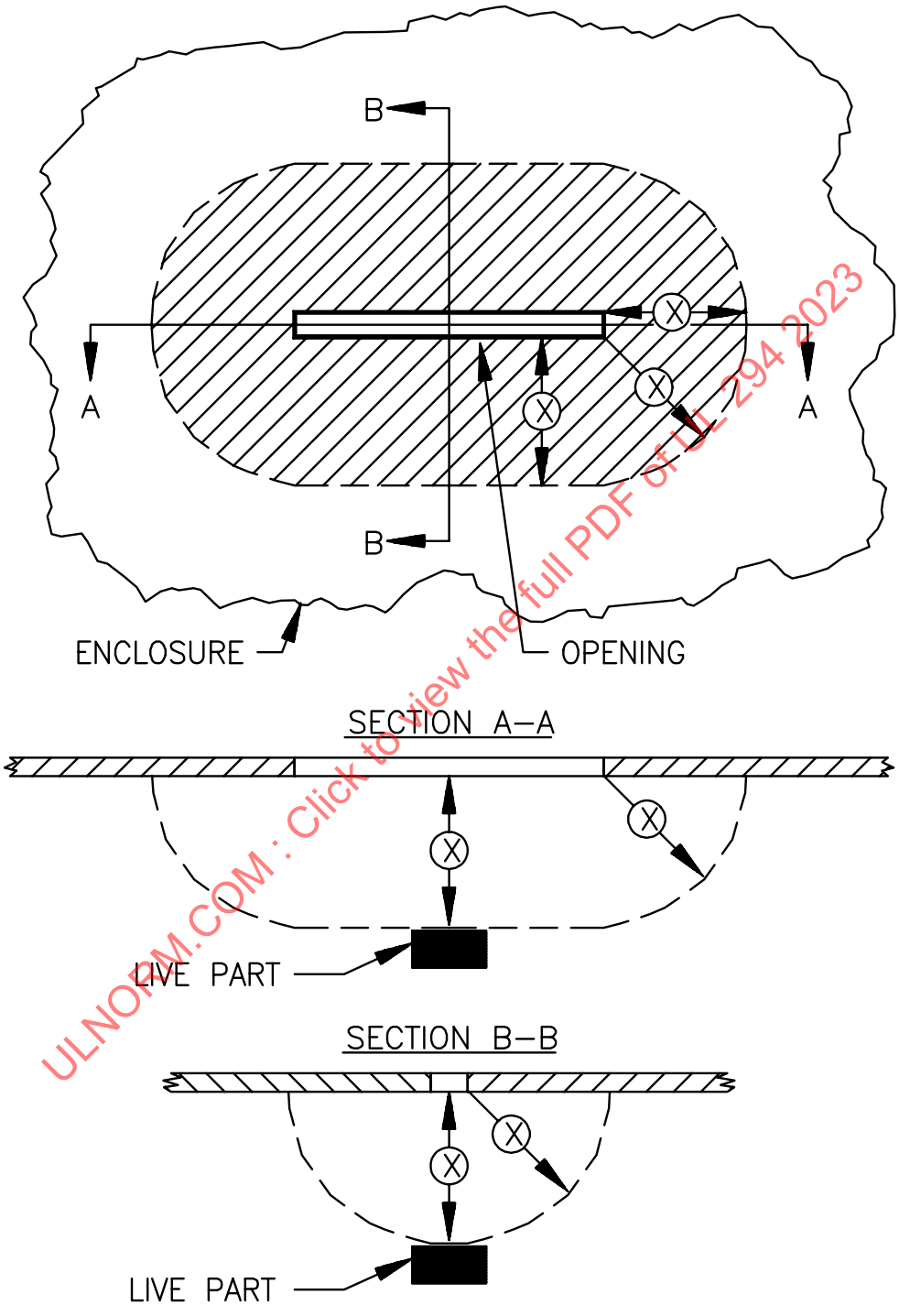


Figure 10.2

Opening in Enclosure



EC100A

NOTE – The opening may be used if, within the enclosure, there is no uninsulated live part or film-insulated wire less than X inches (mm) from the perimeter of the opening, as well as 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 6-1/4 inches (154 mm).