

JUNE 19, 2018

1

UL 293

**Outline of Investigation for Performance of Access Control System Units
Intended for Use in the UK**

Issue Number: 4

June 19, 2018

Summary of Topics

This is the fourth issue of the Outline of Investigation for Performance of Access Control System Units Intended for Use in the UK, UL 293, is being issued to address editorial corrections and to add clarification to requirements. This outline describes the performance test requirements by which access control system units are evaluated for use within UK buildings. The primary purpose of the outline is to enable manufacturers of access control units to satisfy the needs of the Secured by Design initiative (www.securedbydesign.com), which focuses on crime prevention of homes and commercial premises and promotes the use of security standards for a wide range of applications and products. The initiative combines minimum requirements of physical security and well-tested principles of natural surveillance and defensible space.

UL's Outlines of Investigation are copyrighted by UL LLC. Neither a printed nor electronic copy of an Outline of Investigation should be altered in any way. All of UL's Outlines of Investigation and all copyrights, ownerships, and rights regarding those Outlines of Investigation shall remain the sole and exclusive property of UL LLC.

COPYRIGHT © 2018 UL LLC

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents

Document Sharing Hub

No Text on This Page

*UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL*



Documents

Document Sharing Hub

CONTENTS

INTRODUCTION

1 Scope	5
2 General	6
3 Components	7
4 Units of Measurement	7
5 Undated References	7
6 Terminology	7
7 Definitions	7
8 Summarized Access Control Parameter Definitions	10
9 Installation and Operating Instructions	12

CONSTRUCTION & ASSEMBLY

10 Product Assembly	13
11 Test Units and Data	13
12 Test Samples and Miscellaneous Data	13
13 Rechargeable Storage-Type Batteries Used As a Secondary Power Source	14
14 Lithium Batteries	15
15 Essential Computer Equipment	15

PHYSICAL ATTACK PERFORMANCE

16 Destructive/ Manual Attack Test	16
17 Physical Attack Alarm Tests	17

ELECTRICAL PERFORMANCE

18 Normal Operation Test	18
19 Electrical Supervision Test	19
20 Power Interruption Test	20
21 Standby Power Test	20
22 Under Voltage Operation Test	20
23 Over Voltage Operation Test	20
24 Variable Ambient Test	20
25 Humidity Test	21
26 Jarring Test	21
27 Input Measurement Test	22
28 Output Measurement Test	23
29 Overload Test	24
30 Battery Replacement Test	24
31 Endurance Test	25
31.1 General	25
31.2 Separately energized circuits	25
32 Temperature Test	26
33 Electrical Transient Tests	29
33.1 General	29
33.2 Supply line (ring wave surge voltage) transients	30
33.3 Internally induced transients	31
33.4 Input/output (low-voltage) field-wiring transients	31

34 AC Induction Test	36
35 Strain Relief Test	37
35.1 General	37
35.2 Field-wiring leads	38

FITNESS FOR PURPOSE PERFORMANCE

36 Water Ingress	38
------------------------	----

COMMUNICATION SECURITY PERFORMANCE

37 General	38
38 Communication Security for Access Control Level 2	39
39 Communication Security for Access Control Level 3	40
40 Communication Security for Access Control Level 4	40

MARKING

41 General	41
42 Marking Permanency Tests	42
43 Outdoor Use Equipment	43
44 Accessory Equipment	43

APPENDIX A Bibliography

APPENDIX B

Standards for Components.....	B1
-------------------------------	----

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents

Document Sharing Hub

INTRODUCTION

This Outline of Investigation is published by Underwriters Laboratories Inc. at the request of UL LLC. This document is an Outline of Investigation and not a consensus standard; it was not developed as a UL Standard by a UL Standards Technical Panel following UL's accredited consensus process. The technical requirements in this Outline of Investigation have been determined and will be maintained by UL LLC.

This Outline of Investigation is provided "as-is" without representation or warranty of any kind. In publishing and making this document available, Underwriters Laboratories Inc. is not undertaking to render professional or other services for or on behalf of any person or entity, nor undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information.

Underwriters Laboratories Inc. does not undertake to police or enforce compliance with the contents of this document. Underwriters Laboratories Inc. does not certify, test, or inspect products, designs, or installations for safety, health or other purposes. Any certification or other statement of compliance with any requirements in this document shall not be attributable to Underwriters Laboratories Inc. and is solely the responsibility of the certifier or maker of the statement.

1 Scope

1.1 This Outline of Investigation describes the general performance requirements for functionalities of electronic access control systems for use in security applications and products covered by this Outline are intended to be installed in accordance with the Secured by Design HOMES specification. The testing of the components/systems is divided into four areas of performance:

- a) Physical attack;
- b) Electrical performance;
- c) Fitness for purpose; and
- d) Communication security.

1.2 The safety, design, planning, installation, system and equipment maintenance as they relate to risk assessment are not part of this Outline of Investigation. Access control systems and equipment covered by this Outline are intended to be installed in accordance with local and municipal codes and are not intended to impede means of egress.

1.3 An electronic access control system consists of one or more components that when interconnected meet the functionality criteria stated in this Outline.

1.4 This Outline defines different security level designations and the functionalities of the access control system associated with each of these levels.

1.5 The access control system shall also fulfil the relevant requirements of the applicable IEC standards. Functions additional to the mandatory functions specified in this Outline may be included in the electronic access control system providing they do not prevent the requirements of this Outline from being met.

1.6 This Outline also applies to access control systems sharing means of recognition, detection, triggering, interconnection, control, communication, alert signalling and power supplies with other applications. The operation and performance of an access control system should not be adversely influenced by other interconnected applications.

1.7 An electronic access control system may consist of any number of access points. This Outline addresses the security grade classification for each access point and not the overall system.

1.8 Compliance of the individual component parts of the electronic access control system can be assessed to this Outline provided all relevant requirements are applied.

1.9 This Outline defines the minimum requirements as they apply to the components and/or systems, as well as tiered characteristics to meet four levels of security performance with Level 1 (lowest level) to Level 4 (highest level).

1.10 The requirements contained in this Outline do not apply to Video Surveillance systems and computer equipment that, when used as part of the access control system, is necessary to support the operation of the access control system. When Video Surveillance System components are fitted for the basic functionality of the access control system, these components are typically investigated to the requirements of BS EN / IEC 62676-1-1.

1.11 This Outline does not apply to supplementary computer equipment that is not necessary for operation of the access control system if 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.

2 General

2.1 It is recommended that the components and/or system comply with the requirements given in the International Standard for Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements, IEC 60839-11-1, except where the requirements given in this Outline are different, in which case this Outline is deemed to be dominant.

2.2 Biometric equipment parameters such as False Accept Rates, False Reject Rates, Failure to Enroll, Failure to Acquire, etc. are not specifically evaluated as part of this Outline.

2.3 Access control systems that include Hold-Up signaling features are recommended to comply with IEC 62642-1, Alarm systems – Intrusion and hold-up systems – Part 1: System requirements.

2.4 Door locking hardware is recommended to comply with the International Standard for Building hardware – Locks and latches – Mechanically operated locks, latches and locking plates – Requirements and test methods, BS EN 12209, or the International Standard for Building hardware – Locks and latches – Electromechanically operated locks and striking plates – Requirements and test methods, BS EN 14846, as applicable.

2.5 Products intended for installation within air-handling spaces shall also comply with the relevant parts of the UK Building Regulations, Approved Document B (fire safety) Volume 1: Dwelling Houses, and UK Building Regulations, Approved Document P, electrical safety – Dwellings.

2.6 Door entry systems that provide controlled visitor entry into a building at the discretion of the building occupant can be employed in conjunction with the access control system. When a door entry system is used any fault or electrical/mechanical manipulation of the door entry equipment shall not affect the access control system or cause unauthorized entry.

2.7 Physical attack tests included in this document are conducted on equipment that is located on the outside of the restricted or protected area.

3 Components

3.1 A component of a product covered by this Outline shall comply with the requirements for that component. See Appendix B for a list of standards covering components generally used in the systems covered by this Outline.

4 Units of Measurement

4.1 Unless otherwise indicated, all voltage and current values mentioned in this Outline are root-mean-square (rms). Values stated without parentheses are the requirement. Values in parentheses are explanatory or approximate information.

5 Undated References

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

6 Terminology

6.1 The term “product” as used in this Outline refers to all types of access control equipment, components or systems of equipment.

7 Definitions

7.1 For the purpose of this Outline and unless noted otherwise, the definitions given in Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements, IEC 60839-11-1, are also applicable to this Outline.

7.2 ACCESS CONTROL – A means and/or measure to regulate or control physical access 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.

7.3 ACCESS CONTROL MONITORING CONSOLE – Functional component that consists of devices used as control, logging and indicating interface for the operator/ administrator of the electronic access control system.

7.4 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.

7.5 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.

7.6 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.

7.7 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).

7.8 ALARM – A condition requiring human assessment or intervention.

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

7.10 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)

7.11 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.

7.12 COMMUNICATION SECURITY – Equipment that 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.

7.13 COMMUNICATION SECURITY LEVELS –

LEVEL 1 – An access control product with no communication security.

LEVEL 2 – An access control product provided with standard communication security. See Section 42.

LEVEL 3 – An access control product provided with 128 bit encryption and AES or equivalent standards. See Section 43.

LEVEL 4 – An access control product provided with 256 bit encryption and AES or equivalent standards. See Section 44.

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

7.15 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.

7.16 CRITICAL COMPONENT – A critical component is one whose malfunctioning will impair the normal operation of the product, or grants unauthorized access.

7.17 DOOR ENTRY SYSTEMS – A system that provides controlled visitor entry into a building by audio and visual communication between a building occupant and a visitor, and remote release of the primary entrance door locking mechanism from the occupant's dwelling.

7.18 ENDURANCE LEVELS –

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

LEVEL 2 – An access control product shall operate as intended at rated voltage and current for 25,000 cycles of intended operation.

LEVEL 3 – An access control product shall operate as intended at rated voltage and current for 50,000 cycles of intended operation.

LEVEL 4 – An access control product shall operate as intended at rated voltage and current for 100,000 cycles of intended operation.

7.19 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.

7.20 ESSENTIAL COMPUTER EQUIPMENT – Equipment connected to the access control system either on or off premises that is relied upon by the system for access control operations.

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

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

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

7.24 PHYSICAL ATTACK – The ability of the system or, where applicable, the component, to resist attack as specified in EN 1627/EN 1630. When tested in accordance with EN 1630 using the manual attack tool sets and times specified, the test specimen shall not fail at the resistance class claimed.

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

7.26 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.

7.27 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.

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

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

7.30 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.

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

7.32 STANDBY POWER LEVELS –

LEVEL 1 – An access control product designed with no secondary power source.

LEVEL 2 – An access control product that operates as intended, with a loss of primary power for 1 hour while the product is operated every minute.

LEVEL 3 – An access control product that operates as intended, with a loss of primary power for 2 hours while the product is operated every minute.

LEVEL 4 – An access control product that operates as intended, with a loss of primary power for 4 hours while the product is operated every minute.

8 Summarized Access Control Parameter Definitions

8.1 The access control features identified in Table 8.1 shall be identified for the product or equipment by the Level specified by the manufacturer for that feature.

Table 8.1
Summarized access control parameters

Feature	Level 1	Level 2	Level 3	Level 4
Physical attack	No attack test	Withstand attack to RC2 to EN 1627/ EN 1630	Withstand attack to RC2 to EN 1627/ EN 1630 and generates a local alarm before the end of the attack test	Withstand attack to RC2 to EN 1627/ EN 1630 and generates a local alarm before the end of the attack test and signals to a monitoring console.
Communication security	No communication security	Standard communication security	Encrypted communication security – 128 bit	Encrypted communication security – 256 bit
Standby power	No secondary power source	Can maintain normal operation at max load for a minimum of 1 hour	Can maintain normal operation at max load for a minimum of 2 hours	Can maintain normal operation at max load for a minimum of 4 hours
Endurance	1000 cycles	25,000 cycles	50,000 cycles	100,000 cycles
Fitness for purpose	A product or component located on the outside of the protected or restricted area shall comply with the water ingress requirements of Section 40.			

8.2 The security parameters (Levels 1 to 4) chosen for the end-use installation is dependent upon a number of factors such as, which are generally an element of the end-use security vulnerability assessment:

- a) Number of residential units in the property;
- b) Crime levels;
- c) Regional location; and
- d) Occupier demographic.

8.3 The required level of security is beyond the scope of this document as each of the above factors can influence the level required and will vary between properties. The choice of level is therefore outside the scope of this document and is dependent upon the products end use application and risk assessment for the purpose.

8.4 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 41.9.

8.5 The level of access control (Levels 1, 2, 3 or 4) shall be permanently marked on the product or equipment.

9 Installation and Operating Instructions

9.1 A copy of the installation and operating instructions intended to accompany the product and related schematic wiring diagrams and installation drawings are to be provided with the sample submitted for investigation. The instructions, drawings, and diagrams are to be used as guides in the examination and test of the product, and for this purpose need not be in final printed form.

9.2 The installation diagram(s) and any special field installation instructions shall be attached to the unit or, when separate, shall be provided in printed hardcopy format. A copy shall be supplied with each individual product or with each single shipment when multiples of the same products are shipped directly (to an end customer) in a single shipment. If the installation wiring diagram is not affixed to the product, it must be referenced on the product by drawing number and issue date or by model number.

9.3 The following sections contain information that shall be provided in printed hardcopy format and supplied with the unit(s):

- a) 8.1;
- b) 41.1, Exception No. 1;
- c) 41.3;
- d) 41.4; and
- e) 41.8.

9.4 Other installation instructions, operating and test instructions shall be made available by printed hardcopy or by electronic media such as a CD, DVD, official company online portal or website, etc. A copy shall be supplied with each individual product or with each single shipment when multiples of the same products are shipped directly (to an end customer) in a single shipment.

9.5 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.

CONSTRUCTION & ASSEMBLY

10 Product Assembly

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

10.2 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.

10.3 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.

11 Test Units and Data

11.1 Access control equipment units that are fully representative of production units are to be used for each of the following tests unless otherwise specified.

11.2 The devices used for testing are to be those specified by the wiring diagram of the product, except that substitute devices may be used if they produce functions and load conditions equivalent to those obtained with the accessories intended to be used with the product in service.

12 Test Samples and Miscellaneous Data

12.1 The following samples are to be provided for testing:

- a) Two or more complete access control equipment units. However, a single sample may be provided if the size and complexity of the product would make it impracticable to provide more than one sample. The single sample shall be fully representative of the product.
- b) One or more samples of each encapsulated or sealed assembly shall be provided in the un-encapsulated or unsealed condition.
- c) Installation and operating instructions as specified in Section 9, Installation and Operating Instructions.

12.2 One of the following configurations shall be provided for testing:

- a) Samples described in 12.1 with associated access control equipment for testing. The equipment submitted for test shall include the product under test, and any associated equipment to provide a complete access control system for test. All equipment submitted shall be tested without requiring any simulator or other equipment that can emulate any sub-system of the access control system.
- b) Samples described in 12.1 with associated simulator or other equipment that can emulate a specific sub-system of the access control system.

- 1) Any simulator provided shall simulate an interface connection to the product under test.
- 2) Any simulator provided shall completely provide the necessary communication protocols for a published public interface listed in Table 12.1, Test Interfaces.
- 3) Testing shall utilize all parameters of the communications protocols listed in (2).
- 4) The simulator shall not be tested but its implementation of the communications protocols listed in (2) shall be verified.
- 5) Test voltages and transient tests for the product shall still comply.

Table 12.1
Test Interfaces

Interface Description
SIA AC-01-1996.10 – Access Control Standard Protocol for the 26-bit Wiegand Reader Interface
SIA Open Supervised Device Protocol (OSDP), v2.1.5 or later

13 Rechargeable Storage-Type Batteries Used As a Secondary Power Source

13.1 A storage battery shall have sealed cells, or cells with spray trap vents, and shall be maintained in the charged state.

13.2 Batteries shall be located and mounted so that terminals of cells are prevented from coming into contact with terminals of adjacent cells or with metal parts of the battery enclosure as a result of shifting of the batteries.

13.3 The mounting arrangement for the batteries shall permit access to the cells for testing and maintenance, or the product shall provide integral meters or readily accessible terminal facilities for the connection of meters for determining battery voltage and charging current.

13.4 A conditioning charge shall be limited so that, with the maximum rate of charge that can be obtained, the battery gases do not adversely affect any part of the product. The trickle and fast charge rates of a battery shall not exceed the battery manufacturer's recommended rates.

13.5 The battery shall be protected against excessive loading or charging current by a fuse or other overcurrent protective device.

14 Lithium Batteries

14.1 Lithium batteries shall comply with the requirements in the Standard for Lithium Batteries, UL 1642, or the Standard for Household and Commercial Batteries, UL 2054, as applicable.

14.2 A lithium battery shall be protected from abnormal charging currents during use as required.

15 Essential Computer Equipment

15.1 This section describes test methods for the evaluation of essential computer equipment meeting the conditions specified in 15.2. This section does not apply to equipment such as the main access control system unit (dedicated control panel) and card readers.

15.2 Essential computer equipment meeting all the conditions specified in 15.2 (a) – (h) need not be subjected to Sections 22 – 36.

a) Data processing equipment and office appliance and business equipment used as computer equipment shall comply with IEC/UL 60950-1.

b) The manufacturer specifies the minimum system configuration consisting of the following:

- 1) Operating system class, minimum revision levels/or kernel type and revision level.
- 2) Microprocessor type, minimum revision level and minimum clock speed.
- 3) Minimum disk storage.
- 4) Minimum memory requirements.
- 5) Access Control Monitoring software revision level.

c) A product meeting, but not exceeding the specifications of (b), shall be submitted for compliance with the following tests:

- 1) Normal Operation and
- 2) Electrical Supervision.

d) The installation instructions shall specify supply line transient protection complying with the Standard for Surge Protective Devices, UL 1449, with a maximum marked rating of 330 V.

e) The installation instructions shall specify signal line transient protection complying with the requirements for the Standard for Protectors for Data Communication and Fire Alarm Circuits, UL 497B, with the maximum marked rating of 50 V.

f) The installation instructions shall specify that communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors For Communication Circuits, UL 497A. These protectors shall be used only in the protected side of the telecommunications network.