

Australian/New Zealand Standard™

Alarm and electronic security systems

Part 11.1: Electronic access control systems — System and components requirements



AS/NZS IEC 60839.11.1:2019

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee EL-031, Intruder Alarm Equipment and Installations. It was approved on behalf of the Council of Standards Australia on 12 November 2019 and by the New Zealand Standards Approval Board on 4 December 2019.

This Standard was published on 20 December 2019.

The following are represented on Committee EL-031:

- Australian Digital and Telecommunication Industry Association
- Australian Federal Police
- Australian Industry Group
- Australian Security Industry Association
- Engineers Australia
- Fire Protection Association Australia
- Insurance Council of Australia
- New Zealand Security Association
- NSW Police Force
- Queensland Police Service
- Security Providers Association of Australia
- South Australia Police
- Victoria Police
- Victorian Security Institute

This Standard was issued in draft form for comment as DR AS/NZS IEC 60839.11.1:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76072 675 1

Australian/New Zealand Standard™

Alarm and electronic security systems

Part 11.1: Electronic access control systems — System and components requirements

First published as AS/NZS IEC 60839.11.1:2019.

COPYRIGHT

© IEC 2019 — All rights reserved

© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2019

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee EL-031, Intruder Alarm Equipment and Installations.

The objective of this Standard is to specify the minimum functionality, performance requirements and test methods for electronic access control systems and components used for physical access (entry and exit) in and around buildings and protected areas.

This Standard applies to electronic access control systems and components intended to be used in security applications for the granting of access and includes requirements for logging, identification and control of information.

This Standard covers the following:

- (a) A conceptual model and system architecture.
- (b) Criteria covering—
 - (i) classification based on performance functionalities and capabilities;
 - (ii) access point interface requirements;
 - (iii) indication and annunciation requirements (display, alert, logging);
 - (iv) duress signalling and overriding;
 - (v) recognition requirements;
 - (vi) system self-protection requirements; and
 - (vii) communication between the component parts of the electronic access control system and with other systems.
- (c) Requirements for environmental conditions (indoor/outdoor use) and electromagnetic compatibility.
- (d) Test methods.

This Standard does not include requirements for access point actuators and sensors.

This Standard is not intended to cover requirements for off premise transmission associated with intrusion or hold up alarm signals.

This Standard is identical with, and has been reproduced from, IEC 60839-11-1:2013, *Alarm and electronic security systems — Part 11-1: Electronic access control systems — System and components requirements*.

As this document has been reproduced from an International Standard, the following applies:

- (A) In the source text “this part of IEC 60839” should read “this Australian/New Zealand Standard”.
- (B) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

NOTES

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviations	20
5 Conceptual models and system architecture	20
6 System performance functionality requirements.....	23
6.1 Classification methodology and functionalities – Determining the levels of protection	23
6.2 Access point interface requirements	25
6.2.1 Portal release timing.....	25
6.2.2 Access control	25
6.2.3 Portal status	25
6.3 Indication and annunciation (display, alert, logging) requirements	26
6.3.1 Annunciation	26
6.3.2 Display	26
6.3.3 Alert	26
6.3.4 Logging	27
6.4 Recognition requirements.....	29
6.5 Duress signalling requirements	32
6.6 Overriding requirements	32
6.7 Communication requirements	33
6.8 System self-protection requirements.....	33
6.9 Power supply requirements	35
7 Environmental and EMC (immunity) requirements.....	36
8 Test methods.....	38
8.1 General conditions	38
8.1.1 Atmospheric conditions for tests	38
8.1.2 Operating conditions for tests	38
8.1.3 Specimen configuration	38
8.1.4 Mounting arrangements	39
8.1.5 Tolerances	39
8.1.6 Provisions for tests	39
8.1.7 Optional functions.....	39
8.2 Reduced functional test.....	41
8.3 Functional tests for access point interface	41
8.3.1 Object of the test	41
8.3.2 Principle	41
8.3.3 Procedure.....	41
8.3.4 Criteria for compliance.....	43
8.4 Functional tests for indication/annunciation (displaying, alert and logging)	43
8.4.1 Object of the test	43
8.4.2 Principles	43
8.4.3 Test procedure	43
8.4.4 Criteria for compliance.....	46

8.5	Test methods for recognition functionalities	46
8.5.1	Object of the test	46
8.5.2	Principles	47
8.5.3	Test procedure	47
8.5.4	Criteria for compliance.....	48
8.6	Functional tests for duress signalling.....	48
8.6.1	Object of the test	48
8.6.2	Principles	48
8.6.3	Test procedure (ref. Table 5, lines 1 to 3)	48
8.6.4	Criteria for compliance.....	49
8.7	Functional tests for overriding	49
8.7.1	Object of the test	49
8.7.2	Principles	49
8.7.3	Test procedure (ref. Table 6, lines 1 to 7)	49
8.7.4	Criteria for compliance.....	49
8.8	Functional tests for communication and self-protection.....	50
8.8.1	Object of the test	50
8.8.2	Principles	50
8.8.3	Test procedure (ref. Table 7, lines 1 to 28)	50
8.8.4	Criteria for compliance.....	51
8.9	Power supply requirements	51
8.9.1	Test of standby power duration.....	51
8.9.2	Test of charger and standby power source capacity.....	52
8.9.3	Test for low or missing battery condition.....	53
8.10	Environmental and EMC (immunity) tests	53
8.10.1	Test procedure	53
8.10.2	Initial measurements	54
8.10.3	State of the specimen during conditioning	54
8.10.4	Conditioning	54
8.10.5	Measurement during conditioning	54
8.10.6	Final measurements	54
8.10.7	Criteria for compliance.....	54
8.11	Test report	54
9	Documentation and marking	55
9.1	Documentation	55
9.2	Marking	55
Annex A (normative)	Timing diagram	57
Bibliography		58
Figure 1 – Conceptual model	22	
Figure 2 – Typical architecture of an electronic access control system.....	23	
Figure 3 – Example of system test configuration	40	
Figure A.1 – Timing diagram	57	
Table 1 – Grade classification.....	24	
Table 2 – Access point interface requirements	25	
Table 3 – Indication and annunciation requirements	27	

Table 4 – Recognition requirements 30

Table 5 – Duress signalling requirements 32

Table 6 – Overriding requirements 32

Table 7 – System self-protection requirements 34

Table 8 – Power supply requirements 36

Table 9 – Environmental and EMC (immunity) requirements 37

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM AND ELECTRONIC SECURITY SYSTEMS –**Part 11-1: Electronic access control systems –
System and components requirements**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60839-11-1 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this standard is based on the following documents:

FDIS	Report on voting
79/410/FDIS	79/416/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 60839 series, published under the general title *Alarm and electronic security systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is part of the IEC 60839 series, written to include the following parts:

Part 11-1 Electronic access control systems – System and components requirements

Part 11-2 Electronic access control systems – Application guidelines

This part of IEC 60839 describes the general requirements for functionalities of electronic access control systems (EACS) for use in security applications. The design, planning, installation, operation, and maintenance are part of the application guidelines in IEC 60839-11-2¹. The risk analysis is not part of this standard and the risk levels are for informational purposes only.

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

This standard defines different security grades and the functionalities of the access control system associated with each of these grades. It includes also the minimum environmental and EMC compliance criteria as applicable for components of the electronic access control system in every grade.

When a part of an electronic access control system (e.g. access point interface) forms a part of an alarm system (intrusion, hold-up, VSS [Video Surveillance Systems], etc.) that part shall also fulfil the relevant requirements of the applicable IEC standards. Functions additional to the mandatory functions specified in this standard may be included in the electronic access control system providing they do not prevent the requirements of this standard from being met.

This International standard 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 of an access control system should not be adversely influenced by other applications.

An electronic access control system may consist of any number of access points. This standard addresses the security grade classification for each access point.

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

The specific requirements for access point actuators, such as electric door openers, electronic locks, turnstiles and barriers are included in other standards.

¹ Under consideration.

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-1: Electronic access control systems – System and components requirements

1 Scope

This part of IEC 60839 specifies the minimum functionality, performance requirements and test methods for electronic access control systems and components used for physical access (entry and exit) in and around buildings and protected areas. It does not include requirements for access point actuators and sensors.

This standard is not intended to cover requirements for off premise transmission associated with intrusion or hold up alarm signals.

This standard applies to electronic access control systems and components intended to be used in security applications for the granting of access and includes requirements for logging, identification and control of information.

The standard comprises the following:

- A conceptual model and system architecture.
- Criteria covering:
 - classification based on performance functionalities and capabilities;
 - access point interface requirements;
 - indication and annunciation requirements (display, alert, logging);
 - duress signalling and overriding;
 - recognition requirements;
 - system self-protection requirements;
 - communication between the component parts of the electronic access control system and with other systems.
- Requirements for environmental conditions (indoor/outdoor use) and electromagnetic compatibility.
- Test methods.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60068-1, *Environmental testing – Part 1: General and guidance*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 62262, *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)*

IEC 62599-1, *Alarm systems – Part 1: Environmental test methods*

IEC 62599-2, *Alarm systems – Part 2: Electromagnetic compatibility –Immunity requirements for components of fire and security alarm systems*

IEC 62642-1, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

IEC 62642-6, *Alarm systems – Intrusion and hold-up systems – Part 6: Power supplies*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

abnormal status

deviation from the expected mode of operation

3.2

access

physical access

action of entering into (or exiting from) a security controlled area

3.3

access control unit

controller

part of an access control system that interfaces with readers, locking devices and sensing devices, making a decision to grant or deny access through a portal

3.4

access decision

action of comparing information with pre-set rules to determine whether to grant or deny access

3.5

access level

set of rules used to determine where and when a credential has authorized access to one or more portals and which may include special passage conditions such as specific portal allowed open times

3.6

access point

portal

physical entrance/exit at which access can be controlled by a door, turnstile or other secure barrier

3.7

access point actuation

portal actuation

function of an electronic access control system related to the releasing or securing of a portal according to pre-set rules and conditional on the access rights of users

3.8

access point overriding

portal actuation overriding

action of issuing a manual command to bypass the pre-configured mode of operation (i.e. release/secure/block) of an access point

3.9**access point actuator**
portal actuator

part of an access control system that interfaces to an access control unit releasing and securing a portal according to pre-set rules

3.10**access point forced open**
portal forced open

alert signal generated when an access point is opened without access being granted

3.11**access point interface**
portal interface

device or circuitry which controls releasing and securing of an access point

3.12**access point status change**
portal status change

event initiated by the change of an access point either from locked to unlocked or from unlocked to locked

3.13**access point locking device**
portal locking device

assembly associated with the access point, which performs the function of holding an access point in the closed position and capable of releasing the access point in accordance with pre-set rules

3.14**access point open time**
portal open time

maximum time an access point door may be held open after access is granted and before an access point opened too long alert is generated

3.15**access point opened too long alert**
portal opened too long alert

signal generated when an access point open time is exceeded after access is granted

3.16**access point release**
portal release

signal to the access point locking device that access has been granted

3.17**access point sensor**
portal sensor

electrical component used to monitor the open or closed status of an access point, or locked/unlocked status of a locking device, or the secure/unsecure status of an electromagnetic lock or armature plate

3.18**access request**

reading of a credential at a portal initiating the decision process for granting entry to or exit from the area controlled by the portal

Note 1 to entry: See request-to-exit device.

3.19**access request response time**

time required by the system to react to an access request from the correct presentation of the credential until the activation of the responding device

Note 1 to entry: Access request response time replaces the term authentication time.

3.20**accessory equipment**

any component of an electronic access control system other than the access control unit

3.21**alarm**

<access control system> condition requiring human assessment or intervention.

Note 1 to entry: Often used in electronic access control system in the sense of alert.

3.22**alert**

functionality of an electronic access control system related to the activation of an indicator to prompt human assessment

3.23**alert at the portal**

visual and or audible signal at the portal prompting action to close the opened access point/portal and terminate the alert condition

3.24**alert inhibition****by-passing**

system function preventing an event from generating an alert

Note 1 to entry: The alert inhibition event may or may not be logged.

Note 2 to entry: The alert inhibition is manually enabled/disabled by the system operator portal by portal.

3.25**ancillary device**

piece of equipment for supplementary control purposes designed to be attached or added to an electronic access control system by qualified service personnel and which will not prevent the basic access control system requirements from being met

3.26**annunciation**

presentation of the information to users, management or other systems, achieved by the DISPLAY, ALERT and LOGGING functionalities of an electronic access control system

3.27**anti-passback**

operating mode which requires user validation when leaving a security controlled area in order to be able to re-enter and vice versa

Note 1 to entry: Also refer to hard anti-passback, soft anti-passback, global anti-passback, and timed anti-passback.

3.28**area controlled anti-passback**

operating mode which requires the user to be present in a designated security controlled area in order to be able to enter another security controlled area

3.29**anti-passback overriding**
anti-passback disabling

system feature disabling the anti-passback

3.30**anti-tailgating**

function which prevents or detects the attempt of two or more persons or entities to gain access using only one set of credentials

3.31**armature plate**

metal plate designed for use with an electromagnetic lock

3.32**authentication**

process used to verify the integrity of the recognition of credentials

3.33**biometrics****biometric**, adj

any measurable, unique physiological characteristic or personal trait that is used as a credential to recognize and verify the identity of an individual's dynamics

EXAMPLE: Biometrics includes but is not limited to fingerprint, hand or face geometry, retinal/eye, face, voice, signature or keyboarding dynamics.

3.34**blocked access**

passage through an access point is prevented even when valid credentials are presented

3.35**buffered events**

temporarily stored events pending transmission for further processing

3.36**card**

type of token

3.37**cause of denial**

rationale for access denied

EXAMPLE: Causes of denial include: access privilege not including the particular portal, the particular time period, the particular day, the particular holiday, the particular facility code; memorized information incorrect or not provided in time; anti-passback violation; credential expired, not effective or not programmed in the system.

3.38**component**

any part of an electronic access control system

EXAMPLE: Includes access control units, readers, access point actuators, access point sensors, keypads, request-to-exit devices, and any related subassembly.

3.39**configurable**

characteristic of an electronic access control system function to be enabled and disabled or system parameter values to be modified as permitted by pre-set rules

**3.40
configuration**

process or the result of enabling/disabling systems functions and/or changing parameter values as allowed by pre-set rules

**3.41
configuration mode**

state of the access control unit during which the supported system functions can be enabled/disabled or parameters values can be set/changed as required

**3.42
credential**

information either memorized or held within a token

EXAMPLE: The information includes a biometric image used to identify an individual to an access control system in order to authenticate a user

**3.43
credential forgive**

command which re-enables a credential that has violated the anti-passback rules

Note 1 to entry: See forgive and global forgive.

**3.44
credential suspend**

function of an electronic access control system allowing the temporary invalidation of a credential

Note 1 to entry: It is applied on a credential by credential basis, usually in situations when credentials have been lost.

**3.45
credential trace**

function which tracks the movement, in real time, of specific credentials (personal identification numbers, tokens or biometrics) in and out of portals.

Note 1 to entry: Programmed by the system manager the function will cause an alert, log or display on every use of a particular credential (personal identification number, token or biometrics) at any portal as defined by the system manager.

**3.46
credential usage counter**

function used for parking areas and other special applications, which counts the number of uses and determines when the credential expires

**3.47
data authentication**

process used to verify the integrity of transmitted data

Note 1 to entry: Data integrity exists as long as accidental or malicious destruction, modification or removal does not occur.

**3.48
data entry system validation**

system administrator notification of system acceptance/rejection of individual data entered during programming mode

**3.49
deadbolt**

locking device that extends and retracts a bolt using an electrical, hydraulic or pneumatic force

3.50**default**

settings of parameters in the electronic access control system as supplied by the manufacturer that may later be changed

3.51**degraded mode of operation**

limited mode of operation of access control components during communications failure

3.52**delay time for alerting**

time elapsed between the electronic access control system recognizing a change occurring and the related alert being indicated at the monitoring console

3.53**digital inputs**

all inputs to the electronic access control system except communication signals

EXAMPLE: Door monitoring inputs, sensor inputs, inputs from other systems signalling their status, etc.

3.54**display**

functionality of an electronic access control system related to the visual presentation of information within the system

3.55**dual credential****multiple credential**

function of electronic access control systems, which requires two or more sequential authorised access requests within a configurable time period to grant access

3.56**dual occupancy****multiple occupancy**

function of electronic access control systems, which counts the number of users entering and leaving a security controlled area and grants entry/exit only when at least two authorized users enter into/remain in the area at all times

3.57**duress alert**

function of an electronic access control system related to the silent warning initiated by system users entering a duress code when subject to coercive activity in order for unauthorised persons to gain access

3.58**duress signalling**

function of generating a duress alert at the monitoring console

3.59**electric lockset**

mechanical lock designed to also be released electrically

Note 1 to entry: It may also incorporate a mechanical release and an integrated access control unit and/or reader or keypad.

3.60**electric strike**

device controlled remotely which releases the strike plate allowing the portal to open without unlocking the lock

3.61**electric panic bar**

mechanical panic bar designed to also be released electrically

3.62**electromagnetic lock**

electrically powered lock, which locks or unlocks by the activation or deactivation of an electromagnet, magnetically coupled to an armature plate

3.63**electronic access control system
access control system**

system designed to grant to authorized persons, or entities, entry to and/or exit from a security controlled area and deny such entry and/or exit to non-authorized individuals, or entities

Note 1 to entry: The extent of control of entry/exit may include the reporting and recording of related activity.

3.64**elevator control**

function of electronic access control systems restricting the use of lifts or elevator cars

3.65**entity**

any movable object to which access rights has been granted

EXAMPLE: Vehicle, etc.

3.66**event**

change occurring within an electronic access control system

3.67**false acceptance rate**

percentage of erroneous recognition of users where access have been granted

3.68**fault**

condition where any system component fails to perform as designed

3.69**facility code**

number embedded in the token during manufacturing or encoding, to identify the system for which the token is valid

EXAMPLE: System code, site code or customer code.

3.70**forgive**

command given when anti-passback is in use to reset credentials to 'unknown location' status after a hard anti-passback violation

Note 1 to entry: The next time credentials are used, their status is automatically corrected regardless of whether they are used for entry or exit. The command may relate to one credential only (see card forgive) or to all credentials at once (see global forgive) such as following a facility emergency evacuation.

3.71**frame mounted actuator**

frame mounted mechanism, which manipulates a component of a cooperating locking mechanism in a door (such as pushing the latch out of the strike) in response to signals from an input or controlling device allowing the portal to open without unlocking the lock

3.72**free access granting**

condition when a portal is released without decision in accordance with pre-set rules

Note 1 to entry: See also timed free access granting, free access granting until further system command, and single free access granting.

3.73**free access granting until further system command**

system function allowing the system operator to release and re-secure a portal without recognition in accordance with pre-set rules

3.74**global anti-passback**

system feature which applies anti-passback rules at any authorized access point of a controlled area even when the reader is connected to a different access control unit

3.75**global anti-passback credential reactivation**

command given when anti-passback is in use to reset all credentials to 'unknown location' status after a system failure

Note 1 to entry: The next time a credential is used, its status is automatically corrected regardless of whether it is used for entry or exit.

3.76**graphics**

drawings, maps or images providing visible aids used to support the assessment of conditions

3.77**hard anti-passback**

system feature, which generates an alert and denies further access to a particular credential following violation of anti-passback rules

3.78**local time**

time of the country where each access control unit is located

3.79**logging**

function of an electronic access control system related to the recording and retrieving of changes (events) occurring within the system

3.80**logical access levels, pl****access rights, pl**

ability of operators to perform functions within the electronic access control system such as configuration or administration, categorized terms of operator authorization/responsibilities

3.81**man trap**

combination of two or more portals required to be used in sequence in order to gain access to a security controlled area