

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Alarm and electronic security systems –
Part 11-1: Electronic access control systems – System and components
requirements**

**Systèmes d'alarme et de sécurité électroniques –
Partie 11-1: Systèmes de contrôle d'accès électronique – Exigences système et
exigences concernant les composants**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2013 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Alarm and electronic security systems –
Part 11-1: Electronic access control systems – System and components
requirements**

**Systèmes d'alarme et de sécurité électroniques –
Partie 11-1: Systèmes de contrôle d'accès électronique – Exigences système et
exigences concernant les composants**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 13.320

ISBN 978-2-83220-761-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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

Note 1 to entry: The release of a subsequent portal is conditional upon the closure of the previous portal used and upon recognition of valid credentials.

3.82**master clock**

general time synchronising device (clock) of an electronic access control system when there is more than one access control unit

3.83**memorized information**

information known to the user

EXAMPLE: PIN code.

3.84**monitoring console**

functional component that consists of devices used as control, logging and indicating interface for the operator of the electronic access control system

3.85**multiple access****dual access**

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

3.86**normal condition**

access control system that is fully functional and able to process all events according to the pre-set rules

3.87**override, v**

to bypass a function, generally temporarily

EXAMPLE: To temporarily disable the anti-passback function.

3.88**presence check**

confirmation of the number (max., min.) of persons within a security controlled area

3.89**pre-set rules**

set of predefined operating principles by which the electronic access control system functions

3.90**protected area****controlled area**

area defined by a physical boundary, through which passage is controlled by means of one or more access points

3.91**reader**

device for the input of credentials

EXAMPLE: Token reader, card reader, biometric reader, etc.

3.92**reader trace**

function of electronic access control systems allowing the tracking of activities of all credentials for a specific reader

3.93

recognition

action of identifying authorised users requesting access by the comparison of presented credential data with recorded credential data

3.94

release time

period of time access points unlocked by the system according to pre-set rules

3.95

request-to-exit device

device local to an access point used to initiate free exit

3.96

RFID

contactless device for transmitting and/or receiving credential information by radio waves

3.97

roll call

function listing users or credentials recorded as being “IN” the area(s) controlled by the electronic access control system

3.98

scheduled access

timed free access

period of time during which an electronic access control system does not control access or exit as determined by pre-set rules

3.99

single free access granting

system function allowing the system operator to release a portal without credential recognition

Note 1 to entry: Upon closing, the portal is automatically secured by the system in accordance with pre-set rules.

3.100

singularization

limitation to one user passing the access point at the same time

3.101

soft anti-passback

system feature, which, upon granting access, generates only an alert following violation of anti-passback rules

3.102

stand-alone mode

mode of operation of the access control system without the communication between the access control unit and monitoring console

3.103

supervisor mode

function of electronic access control systems which requires a supervisor authorised access request to be used in conjunction with another credential in order to grant access

3.104

system administrator

person with the responsibility of deciding and/or implementing the electronic access control system processing rules

3.105**system defined**

options of electronic access control systems that are set to a fixed value (i.e. factory programmed) that cannot be changed in the field by reprogramming

3.106**system operator**

person with the responsibility of manning the electronic access control system monitoring console who performs monitoring duties and may or may not enter/edit system data

3.107**system self-protection**

functionality of an electronic access control system related to the prevention, detection and/or reporting of deliberate and/or accidental tampering and/or interfering with system operation

3.108**tailgating**

person or entity, passing through an access point without using credentials by following a person or entity for whom access has been granted

3.109**tampering protection**

method used to protect an access control system or part thereof against deliberate interference

3.110**timed anti-passback**

system feature which traces an individual credential access request to a given area for which an access granted was not followed by an exit granted, or an exit granted was not followed by an access granted within a predetermined time period

Note 1 to entry: This feature prevents a second subsequent access request from being authorized to the same card into the same area, prior to the expiration of a user configurable anti-passback time.

3.111**timed free access granting**

selectable time zone when the condition of portal release without credential recognition is permitted

3.112**time slot**

interval of time between two given moments indicating the beginning and the end of a valid period within a time zone

3.113**time zone**

one or more time slots combined with calendar information

3.114**token**

portable device containing a readable unique identifier (credential) that can be associated with a user's data and access rights stored within the electronic access control system

3.115**transaction**

event which corresponds to the release of an access point following recognition of a user identity

3.116

turnstile

portal designed to physically limit passage to only one person at a time

3.117

user

person requesting access through an access point

3.118

identification information

user identity

information which is transferred directly or via token by the user to the recognition equipment

3.119

visitor escorted access

function of electronic access control systems which grants access to an area to a given access level conditional on the sequential use of credentials of a different and specific access level

4 Abbreviations

For the purposes of this document, the abbreviations given in IEC 62642-1 and the following apply.

ACS	Access control system
ACU	Access control unit
APS	Access point sensor
EACS	Electronic access control system
EEPROM	Electrically-erasable programmable read-only memory
FAR	False acceptance rate
ID	Identification information
RAM	Random access memory
REX	Request-to-exit device
RFID	Radio frequency identification or radio frequency identification device

5 Conceptual models and system architecture

The electronic access control system shall include as appropriate to the specific configuration of the access control system the following basic functions: processing (A), communication (B), configuration (programming) (C), access point interface (D), recognition (E), annunciation (F), duress signalling (G), interfacing with other systems (H), self-protection (I), power supply (J), user interface (K):

- A Processing: the comparing of changes occurring within the system with pre-set rules to produce predefined actions.
- B Communication: transmission of signals between components of the access control system to ensure the application of pre-set rules.
- C Configuration (programming): the setting of processing rules.

D Access point interface:

- access point actuation: the portal releasing and securing according to pre-set rules;
- access point monitoring: the continuous reporting of the opened/closed status of the portal, and/or of the releasing/securing status of portal locking devices;
- access point actuation overriding: the releasing/securing of portal according to pre-set rules without recognition.

E Recognition: the recognizing of authorized users requesting access.**F Annunciation: the alert, display and/or logging functionalities:**

- alert: the annunciation sub-functionality related to the activation of an indicator to prompt human assessment;
- display: the annunciation sub-functionality related to the visual and/or audible presentation of changes occurring within the system;
- logging: the annunciation sub-functionality related to the logging and retrieving of changes occurring within the system.

G Duress signalling: the silent warning by system users of on-going coercive access request conditions.**H Interface with other systems: the sharing of functionalities and/or changes occurring within systems.****I System self-protection: the prevention, detection and/or reporting of deliberate and accidental tampering and/or interfering with system operation.****J Power supply: module supplying power to the access control system. The power supply requirements in this standard do not cover the power needs for access point actuators. When a part of an electronic access control system (e.g. access point interface) also forms a part of an intruder alarm system, the power supply of that part shall comply with the relevant requirements of IEC 62642-6.****K User interface: means by which the user requests access (e.g. keypad or token reader) and receives indication of access status.**

Functions additional to the mandatory functions specified in this standard may be included in the electronic access control system providing they do not influence the correct operation of the mandatory functions.

The conceptual model of electronic access control systems and the system architecture are illustrated by Figure 1 and Figure 2.

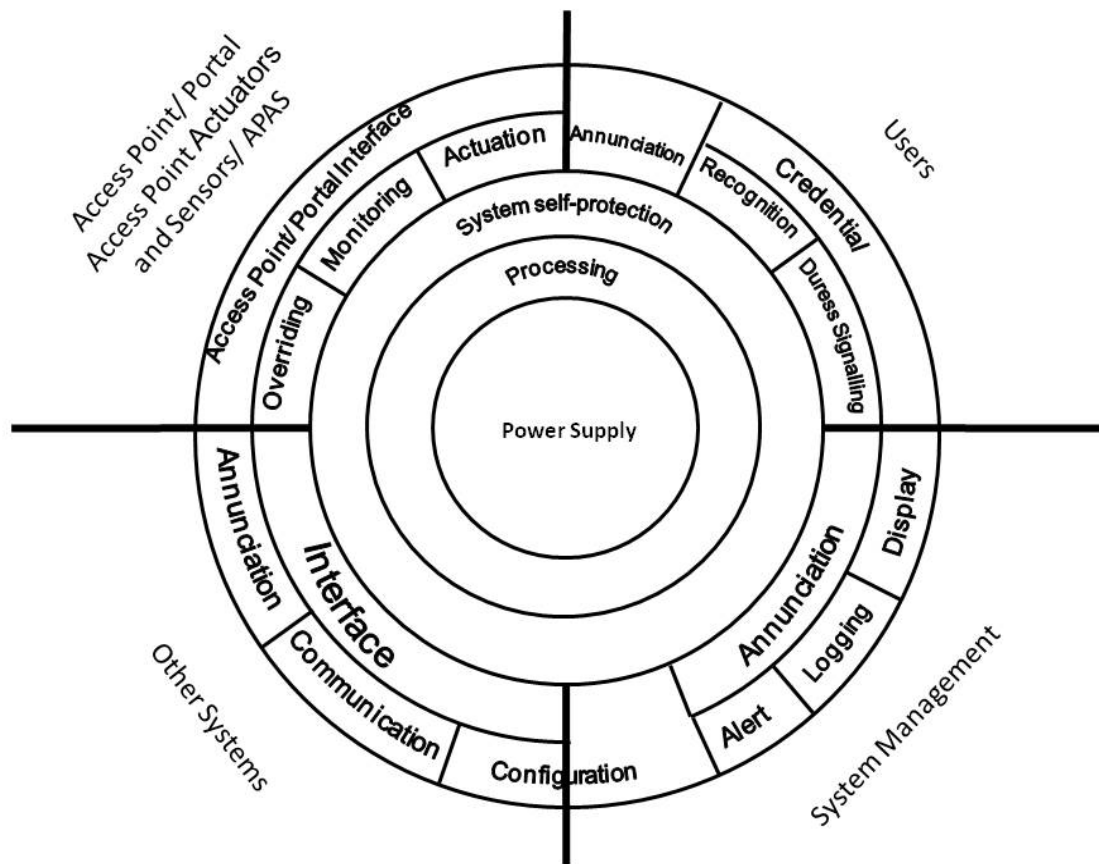
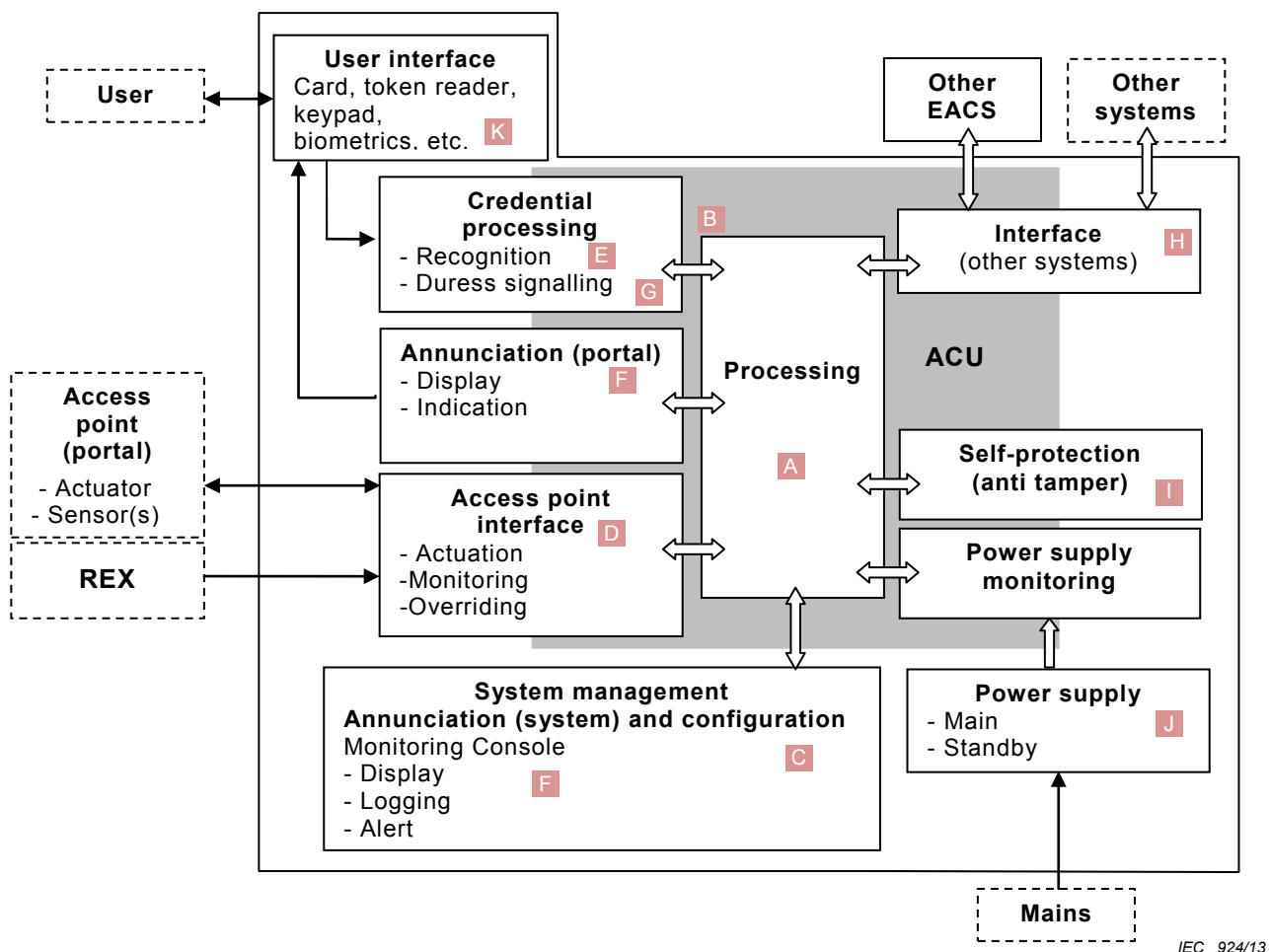


Figure 1 – Conceptual model

IEC 923/13



Components surrounded by dotted lines are not within the scope of this standard.

Functions may be distributed and may be located in more than one enclosure or integrated into a single cabinet.

System management annunciation and configuration may be performed by software applications only. The minimum requirements for the hardware platform shall be specified.

Figure 2 – Typical architecture of an electronic access control system

6 System performance functionality requirements

6.1 Classification methodology and functionalities – Determining the levels of protection

The equipment performance requirements shall be structured according to grades corresponding to levels of protection. This is achieved by classifying the security related functionalities (recognition, access point actuation, access point monitoring, duress signalling and system self-protection) in relation to risk levels.

The classification of the access control system shall be one of the four grades with Grade 1 being the lowest and Grade 4 the highest. The security classification shall be defined for each access point for entry and exit individually (see Table 1).

Different grades for access point interfaces can be used in the same installation as long as the functions provided by the access control system and credentials used fulfil at least the requirements of the highest security classification of access point(s) controlled by that system.

When a function is included that is optional in the standard for the grade to which the component claims compliance, documentation should clearly and explicitly state which, if any, higher grade(s) such functions are compliant with. If such functions are not compliant with the requirements of a higher grade then this shall be clearly and explicitly stated in the documentation.

The risk levels are defined in terms of the value of the assets requiring protection and the determination (knowledge/skills) and methods of attack of persons intending to bypass the system (adversaries).

- Grade 1: low risk. The adversary is expected to have little knowledge of the access control system and be restricted to a limited range of easily available tools. The objective of the physical security is to deter and delay adversaries. Assets have limited value and adversaries in presence will probably give up the idea of attacking when confronted with minimum resistance.
- Grade 2: low to medium risk. The adversary is expected to have limited knowledge of the access control system and the use of a general range of tools and portable instruments. The objective of the physical security is to deter, delay and detect adversaries. The assets have higher value and adversaries in presence will likely give up the idea of succeeding when they realize they may be detected.
- Grade 3: medium to high risk. The adversary is expected to be conversant with access control system and have a comprehensive range of tools and portable electronic equipment. The objective of the physical security is to deter, delay, detect and help identify adversaries. The assets have high value and adversaries in presence may give up the idea of succeeding when they realize they may be identified and caught.
- Grade 4: high risk. The adversary is expected to have the ability or resources to plan the attack in detail and have a full range of equipment including means of substitution of components in the access control systems. The objective of the physical security is to deter, delay, detect and help identify adversaries. The assets have very high value and adversaries in presence may give up the idea of succeeding when they realize they will be identified and caught.

Table 1 – Grade classification

Grade	1	2	3	4
Risk level	Low	Low to medium	Medium to high	High
Application	organizational aspects, protection of low value assets	organizational aspects, protection of low to medium value assets	fewer organizational aspects, protection of medium to high value commercial assets	mainly protection of very high value commercial or critical infrastructure
Skill/ knowledge of adversaries/ attackers	low skill, low knowledge of ACS, no knowledge of token and IT technologies low financial means for attacks	medium skill and knowledge of ACS, low knowledge of token and IT technologies low to medium financial means for attacks	high skill and knowledge of ACS, medium knowledge of token and IT technologies medium financial means for attacks	very high skill and knowledge of ACS, high knowledge of token and IT technologies high financial means for attacks
Typical examples	hotel	commercial offices, small businesses	industrial, administration, financial	highly sensitive areas (military facilities, government, R&D, critical production areas)

6.2 Access point interface requirements

6.2.1 Portal release timing

The access control unit shall be capable of unlocking portals in accordance with pre-set rules for a period of time either system-defined or system-programmable in accordance with Table 2. If the access point status is monitored then the release of the access point actuator shall cease when the access point is opened.

6.2.2 Access control

An electronic access control system shall be capable of controlling access in accordance with Table 2 and the timing diagram presented in Annex A. The requirements of Table 2 shall be applied to individual access points according to their grade. "Global" features shall be applied to all access points of the same grade.

Electronic access control systems should incorporate outputs capable of operating electromagnetic locks, electric strikes, frame mounted actuators, electrical, hydraulic or pneumatic deadbolts, and/or other types of electric locksets and electric panic bars.

6.2.3 Portal status

6.2.3.1 Grade 2

Equipment shall be capable of monitoring the status of portals in accordance with system-defined pre-set rules or be configurable. Should the pre-set rules be system-defined, the permitted portal open time shall not be less than 10 s.

6.2.3.2 Grade 3 and Grade 4

Equipment shall be capable of monitoring the status of portals, and the permitted portal open time shall be in accordance with pre-set rules that are configurable.

Table 2 – Access point interface requirements (1 of 2)

Access point interface requirements		Grade assignment			
		1	2	3	4
A – Release timing					
1	The release time shall be system-defined	OP*	OP*	NP	NP
2	The release time shall be configurable per portal	OP*	OP*	M	M
3	When the release time is system-defined, the permitted value shall not be less than 3 s	M	M	N/A	N/A
4	When the release time is configurable, several permitted values can be associated to access rights per portal	OP	OP	OP	OP
B – Access control					
5	Provide access control for entry into a protected (controlled) area	M	M	M	M
6	Provide access control for exit from a protected (controlled) area	OP	M	M	M
7	Hard anti-passback	OP	OP	M	M
8	Soft anti-passback	OP	OP	OP	OP
9	Global anti-passback	OP	OP	OP	M
10	Anti-passback override/disabling	OP	OP	OP	M
11	Timed anti-passback	OP	OP	OP	M
12	Access granted conditional upon effective/expiry date	OP	OP	M	M
13	Access granted conditional upon credential validity (blocked, suspended, invalid)	M	M	M	M
14	Visitor escorted access	OP	OP	OP	OP

Table 2 (2 of 2)

Access point interface requirements		Grade assignment			
		1	2	3	4
15	Supervisor mode	OP	OP	OP	OP
16	Dual occupancy (two or more persons presence check)	OP	OP	OP	OP
17	Dual access (two-person access)	OP	OP	OP	M
18	Singularization/ anti-tailgating	OP	OP	OP	OP
19	Elevator control	OP	OP	OP	OP
C – Access point status monitoring					
20	Access point/ status shall be monitored	OP	M	M	M
21	Access point permitted open time shall be system-defined (recommended open time to be not less than 10 s)	OP	OP*	NP	NP
22	Access point open time shall be configurable per portal	OP	OP*	M	M
23	When configurable, several permitted open times may be associated with access rights per access point	OP	OP	OP	OP
D – Input signals					
24	Digital input signals (i.e. other than communication signals) with an active period exceeding 400 ms shall be processed	OP	M	M	M
NOTE Abbreviations used in the table are the following: NP = not permitted OP = optional M = mandatory OP* = one of the options in the identified grouping (gray area) shall be implemented N/A = not applicable					

6.3 Indication and annunciation (display, alert, logging) requirements

6.3.1 Annunciation

Electronic access control systems with monitoring console shall be capable of displaying, alerting and logging changes at the monitoring console in accordance with 6.3.1, second paragraph through 6.3.4, second paragraph.

The information provided in accordance with 6.3.1 shall include the type of event, its location, time and date of occurrence.

6.3.2 Display

Electronic access control systems shall be capable of monitoring and displaying events and information at the monitoring console in accordance with Table 3.

Information indication at the portal shall be in accordance with the requirements in Table 3.

6.3.3 Alert

Electronic access control systems shall be capable of activating indicators at the monitoring console to prompt operator assessment of events in accordance with Table 3.

Electronic access control systems shall be designed to process alert signals in accordance with Table 3.

6.3.4 Logging

Electronic access control systems shall log events and information in accordance with Table 3.

Access to the logged information shall be restricted by operator rights.

Table 3 – Indication and annunciation requirements (1 of 3)

Indication and annunciation requirements		Indication			Grade assignment			
					1	2	3	4
A – Portal (local indication)								
1	Visual and/or audible indication required when access is granted	•			M	M	M	M
2	Visual and/or audible indication required when access is denied	•			M	M	M	M
3	Visual and/or audible indication of portal locked status until access is granted	•			OP	OP	OP	OP
4	Visual and/or audible indication is required for the last time period (pre-alert time) of the maximum permitted portal open time if portal remaining open, to warn user(s) that the portal open time is running out. To cease when the portal is closed. Pre-alert time shall be system wide defined or configurable portal by portal (recommended default: 10 seconds)	•			OP	OP	M	M
B – Monitoring console (annunciation)								
		Display	Alert	Logging				
5	Visual annunciation is required when access is granted	•			OP	OP	OP	OP
6	Logging is required when access is granted			•	OP	OP	M	M
7	Visual annunciation, alert and logging required for duress conditions	•	•	•	OP	OP	OP	M
8	Card usage counter	•		•	OP	OP	OP	OP
9	Visual annunciation, alert and logging required for denial of access due to an attempt to use a token with expired validity	•	•	•	OP	OP	OP	M
10	Visual annunciation, alert and logging required for denial of access due to a configurable number of attempts to use a valid token with invalid memorized information. Where the number of attempts is not configurable it shall be limited to 5	•	•	•	OP	OP	OP	M
11	Visual annunciation, alert and logging required for denial of access due to a configurable number of sequential attempts to use invalid memorized information (i.e. the use of PIN only for recognition). Where the number of attempts is not configurable it shall be limited to 5 subsequent attempts within 30 s each	•	•	•	OP	OP	NP	NP
12	Visual indication of access points alerts on the floor plan of the controlled areas	•			OP	OP	OP	M
13	Instructions shall be displayed following alerts	•			OP	OP	OP	M

Table 3 (2 of 3)

Indication and annunciation requirements		Indication			Grade assignment			
					1	2	3	4
B – Monitoring console (annunciation)								
		Display	Alert	Logging				
14	Transactions			•	OP	M	M	M
15	Visual annunciation and logging for portal open status following access granted. It may be configurable by portal in accordance with the grade requirement.	•		•	OP	OP	M	M
16	Visual annunciation, alert and logging for portal remain closed status following access granted. It may be configurable by portal in accordance with the grade requirement	•	•	•	OP	OP	OP	M
17	Access denied. It may be configurable by portal in accordance with the grade requirement	•	•	•	OP	OP	M	M
18	Cause of access denial. It may be configurable by portal and/or cause of denial in accordance with the grade requirement	•	•	•	OP	OP	OP	M
19	Scheduled or manual portal status change			•	OP	OP	M	M
20	Primary power failure	•	•	•	OP	OP	M	M
21	Primary power restoration	•		•	OP	OP	M	M
22	Standby power supply trouble condition (low battery voltage level and no battery present)	•	•	•	OP	OP	M	M
23	Entering and leaving configuration mode	•		•	OP	OP	M	M
24	Loss of communication between access control unit and monitoring console	•	•	•	OP	M	M	M
25	Roll call	•		•	OP	OP	M	M
26	Portal closed following portal forced open or portal opened too long	•		•	OP	OP	M	M
27	All events shall be identified by type, location, time and date of occurrence	•		•	OP	OP	M	M
28	Alerts shall contain an indication of their respective priority level if the system allows assigning of such priority levels	•		•	OP	OP	M	M
29	Concurrently received alerts shall be displayed by order of priority if the system allows assigning of such priority levels	•			OP	OP	M	M
30	Tamper detection	•	•	•	OP	M	M	M
31	Portal forced open	•	•	•	OP	M	M	M
32	Visual annunciation, alert and logging for expiry of portal allowed open time (portal opened too long)	•	•	•	OP	M	M	M
33	Card trace	•		•	OP	OP	OP	M
34	Reader trace	•		•	OP	OP	OP	M
35	Reader condition off-line	•	•	•	OP	OP	OP	M
36	Locking device abnormal status	•	•	•	OP	OP	OP	M

Table 3 (3 of 3)

Indication and annunciation requirements		Indication			Grade assignment			
					1	2	3	4
B – Monitoring console (annunciation)								
		Display	Alert	Logging				
37	Annunciation of reaching the limit of 90 % from maximum logging capacity	•	•	•	OP	OP	M	M
38	Maximum delay time for signals reaching the monitoring console (90 s, 45 s and 15 s)	•	•	•	OP	90 s	45 s	15 s
39	Maximum delay time for displaying text instructions following alert reaching the monitoring console (5 s)	•	•		OP	OP	OP	M
40	Maximum delay time for displaying image and graphics following alert reaching the monitoring console (6 s)	•	•		OP	OP	OP	6 s
41	System shall be capable of assigning priority levels to specific alert events	•			OP	OP	M	M
42	Alerts received at the monitoring console require acknowledgement by the operator	•	•	•	OP	OP	M	M
43	Visual annunciation, alert and logging are required when dual/multiple occupancy conditions are not respected (minimum number of persons not present)	•	•	•	OP	OP	OP	OP
44	All operator initiated changes shall be logged with type, operator ID, time and date of the occurrence			•	OP	OP	OP	M
45	Operator comments to alerts shall be logged with operator ID, time and date of entering the comment. The specific alert covered by the comments shall be identified	•		•	OP	OP	OP	M
46	Accessing logged information for retrieving (e.g. displaying, printing, exporting) events shall be logged with operator ID, time and date of occurrence			•	OP	OP	M	M
47	Minimum number of system events logging capacity on average per reader			•	OP	200	500	1 000
NOTE Abbreviations used in the table are the following: NP = not permitted OP = optional M = mandatory OP* = one of the options in the identified grouping (gray area) shall be implemented N/A = not applicable								

6.4 Recognition requirements

The control of access is a person related application which assigns access rights to individual users or a group of users. The correct recognition of the users is the primary function of the electronic access control system, therefore the selection of user credentials shall be in accordance with the grade (security level) wanted:

- 1) the electronic access control systems shall provide recognition in accordance with Table 4;
- 2) the electronic access control systems shall compare each memorized information with stored credentials to accept or deny users' identity claim;

- 3) the access control unit shall include a real-time clock with the accuracy of ± 10 s a week and capable of adjusting to daylight saving time and leap year, and of managing national time zones as indicated in Table 4. In addition, when multiple access control units are used, the clocks for Grade 3 and Grade 4 equipment shall be synchronized with the master clock at least once every 24 h;
- 4) Grade 2, Grade 3 and Grade 4 electronic access control units shall provide a unique identity to each authorized user;
- 5) the access control unit shall provide a minimum number of user access levels as per Table 4;
- 6) the access control unit shall provide a minimum number of system-programmable time periods as per Table 4;
- 7) the time resolution shall include day of week, hour and minute of the day;
- 8) in addition to item 7) above, the time resolution for Grade 3 and Grade 4 equipment shall include day of the month, month, and year;
- 9) the access control unit shall provide a minimum number of system-programmable holidays as per Table 4.

Table 4 – Recognition requirements (1 of 2)

Recognition requirements		Grade assignment			
		1	2	3	4
A – Access levels					
1	The built-in real time clock shall have an accuracy of ± 10 seconds a week and be capable of adjusting to daylight saving time, leap year	OP	M	M	M
2	The system shall be capable of managing multiple time zones	OP	OP	OP	OP
3	For systems with multiple interconnected control units, the clocks shall be synchronized with the master clock or other reliable synchronization source, at least once every 24 h	OP	OP	M	M
4	Synchronize the master clock of the system to the official time	OP	OP	OP	M
5	Real time clock shall be kept for the indicated minimum period of time in case of total power loss (except for loss of data retention battery)	OP	24 h	120 h	120 h
6	Minimum number of user access levels	1	8	16	64
7	Minimum number of configurable time periods	0	4	8	16
8	Minimum resolution for time within access level includes day of week, hour and minute of day	N/A	M	M	M
9	Minimum resolution for time within access level includes day of month, month and year	N/A	OP	OP	M
10	System shall be capable to handle a number of configurable days (e.g. statutory holidays, special business days and non-business days)	N/A	2	16	24
11	System should be capable of assigning access rights to a group of credentials	OP	OP	OP	OP
12	System should be capable of changing access rights to a group of credentials in response to emergency conditions	OP	OP	OP	OP

Table 4 (2 of 2)

Recognition requirements		Grade assignment			
		1	2	3	4
B – Equipment and methods of recognition					
13	The system shall assign unique identity to each authorized user	OP	M	M	M
14	The system shall use memorized information only	OP*	OP*	NP	NP
15	The system shall use biometrics alone or in combination with other recognition methods	OP*	OP*	OP*	OP*
16	The system shall use token	OP*	OP*	OP*	OP*
17	The system shall use memorized information and token	OP*	OP*	OP*	OP*
18	Access shall be denied after each attempt to gain access using a valid token with invalid memorized information, and after a predetermined number of unsuccessful attempts the access rights for that token shall be suspended for a pre-set duration. The number of attempts can be configurable. Where it is not configurable the number of attempts shall be limited to 5	OP	M	M	M
19	Access shall be denied after each attempt to gain access with invalid memorized information only. The access shall be suspended after 5 sequential incorrect inputs within a pre-set period of time.	OP	OP	N/A	N/A
20	When using biometrics, FAR_{eff} shall not exceed limits shown for each grade. NOTE 1 $FAR_{eff} = FAR$ (false acceptance rate) when 1:1 comparison is performed (e.g. biometric verification of an identity claimed by memorized information or token) or $FAR_{eff} = FAR \times n$ when 1:n comparison is performed and n = number of stored templates (e.g. biometric identification without using memorized information or token). NOTE 2 The FAR values are based on the review of the supplied manufacturer's documentation.	1 %	0,3 %	0,3 %	0,1 %
21	The minimum ratio between number of possible user codes and number of allocated codes shall be at least 1 000 to 1 when system is using recognition of a valid user by memorized information only e.g.: up to 10 users – 4 digits, up to 100 users – 5 digits, up to 1 000 users – 6 digits, etc	M	M	N/A	N/A
22	For systems using recognition by memorized information combined with token or biometrics the memorized information requires 4 digits minimum	OP	OP	M	M
23	In normal mode of operation the system shall use complete token information (facility code and card number, or unique card number) for recognition	M	M	M	M
24	Support for multiple facility codes if the system utilizes facility coding	OP	OP	OP	M
25	In degraded mode of operation the system may use partial token information (e.g. facility code only) for recognition	OP	OP	OP	NP
26	Tokens with coding system structure visible to unaided human eye shall not be used	M	M	M	M
27	The token identity number readable on the token not to be a direct representation of the entire coding	M	M	M	M
NOTE Abbreviations used in the table are the following: NP = not permitted OP = optional OP* = one of the options in the identified grouping (gray area) shall be implemented. Also refer to the additional token requirements for each grade as per item 9) in 6.8 M = mandatory NA = not applicable					

6.5 Duress signalling requirements

The operation of the duress initiating device in the protected area and transmission of an alert to the monitoring console shall be in accordance with Table 5 and the requirements below:

- 1) The duress signal received at the monitoring console shall include identification of location, time and date of occurrence.
- 2) The duress signal received at the monitoring console shall include user identification.

Table 5 – Duress signalling requirements

Duress signalling requirements		Grade assignment			
		1	2	3	4
1	Enabling of the duress functionality shall be configurable	OP	OP	OP	M
2	The duress alert at the monitoring console to be distinct from other alerts	M*	M*	M*	M
3	The operation of the duress initiating device shall not produce a signal which may be audible or visible at the location where the duress has been initiated	M*	M*	M*	M
NOTE Abbreviations used in the table are the following: OP = optional M = mandatory M* = mandatory only if optional functionality is supported for the specified grade					

6.6 Overriding requirements

Electronic access control systems shall allow manual commands that override the configured mode of operation of access point (release/secure/block) in accordance with Table 6 and the requirements below:

- 1) All overriding commands shall be logged with time and date of the occurrence.
- 2) The logged information shall include the type of overriding command and operator ID.

Table 6 – Overriding requirements

Overriding requirements		Grade assignment			
		1	2	3	4
1	Single free access granting, single portal	OP	OP	M	M
2	System-wide free access granting	OP	OP	OP	OP
3	Free access granting until further system command, single portal or group of portals	OP	OP	OP	OP
4	Scheduled/timed free access granting, single portal or group of portals	OP	OP	OP	OP
5	The electronic access control system shall not prohibit the free exit granted by other emergency systems (e.g. fire, environmental)	M	M	M	M
6	Blocking of portal until further system command, single portal or group of portals	OP	OP	OP	OP
7	Scheduled/timed blocking of portal, single portal or group of portals	N/A	OP	OP	OP
NOTE Abbreviations used in the table are the following: OP = optional M = mandatory M* = mandatory only if optional functionality is supported for the specified grade N/A = not applicable					

6.7 Communication requirements

The communication channel between the electronic access control system and the monitoring console shall meet the following requirements:

- 1) Failure and/or restoration of the communication channel for Grade 2, Grade 3 and Grade 4 equipment shall not result in the release of portals.
- 2) The end to end communication verification (timing) shall be conducted as part of the final installation and it shall meet the requirements of Table 3, line 38, for that installation.
- 3) Grade 2, Grade 3 and Grade 4 equipment shall be capable of operating in stand-alone mode after communication interruption with the monitoring console. The equipment shall be capable of performing all functionalities with the exception of the ones affected by the loss of communication.
- 4) Grade 4 equipment shall ensure the integrity of communications between all components of the access control system transmitting or receiving data related to the granting of access, including for example: communications between token/cards and user interfaces, user interfaces and access control units and between access control units and the monitoring console.
- 5) The integrity of communication shall be achieved by supervision of the communication channel (Table 7, line 9) and the security of information transmitted.
- 6) The information security shall be provided by measures to prevent unauthorised reading and modification of the information transmitted.
- 7) Description of how the measures for security of information are achieved shall be provided during testing of the equipment.

6.8 System self-protection requirements

The components of the electronic access control system shall meet the following requirements and the appropriate requirements in Table 7 for each grade.

- 1) The housings for components of electronic access control systems shall be provided with the means to prevent access to internal elements to minimize the risk of tampering. Requirements for tamper protection may vary depending on the grade of the EACS and on whether a component of the system is located within or outside of the protected area.
- 2) Components located externally to the protected area shall have appropriate means of tamper protection and detection as per Table 7, lines 5 and 6.
- 3) All terminals and means of mechanical and electronic adjustment shall be located within electronic access control component housings.
- 4) Open or short circuit conditions applied to wires connected to any components of an access control system installed outside its controlled area or accessible from outside its controlled area shall not result in the operation of the access point actuator device allowing access to the secured area.
- 5) Housing shall be sufficiently robust to prevent undetected access to internal elements without visible damage. The user interface (e.g. reader, keypad, etc.) housing shall be protected to IP4X. It shall not be possible to grant access by the insertion of a 1 mm steel probe into the housing. IP ratings are detailed in IEC 60529.
- 6) The user interface housing shall be protected to IK04. Damage to the housing is permitted after impact, provided that it is not possible to grant access by manipulating internal elements of the user interface. Alternatively a tamper condition shall be generated before access to internal elements is possible. IK ratings are detailed in IEC 62262.
- 7) Means of access to internal elements of components of electronic access control system shall be robust and mechanically secured. Normal access shall require the use of a tool.
- 8) Interconnections shall be suitable for the purpose and designed to provide a reliable means of communication between components of electronic access control system. They shall be designed to minimize the possibility of signals being delayed, modified, substituted or lost.

- 9) The following requirements for token and communication between token and user interface unit shall be met in addition to the requirements stated in Table 4 and Table 7:
- a) Grades 1 and 2: no additional requirements;
 - b) Grade 3: chip based contact or contactless (RFID) token with access conditions at least for writing/modifying of ID information and for RFID token only session encrypted data communication. This is required only when the token is used as a single method of recognition;
 - c) Grade 4: chip based contact or contactless (RFID) token with mutual authentication and access conditions for reading, writing or modifying information and for RFID token only session encrypted data communication.

Table 7 – System self-protection requirements (1 of 2)

System self-protection requirements		Grade assignment			
		1	2	3	4
A – Prevention					
1	Memory stored information (settings) shall be kept for the indicated minimum period of time in case of total power loss (except for loss of data retention battery)	10 min	2 wks	2 wks	2 wks
2	Following a total loss of power automatic restart of the access control system is required upon primary power source restoral	M	M	M	M
3	If full functionality of the access control unit cannot be restored (data corrupted or lost) following the automatic restart a trouble condition shall be annunciated	M	M	M	M
4	Means of access to the internal elements of components of an access control system shall require the use of a tool	M	M	M	M
5	Opening of the enclosure of the user interface intended to be installed outside of the controlled area or that could be accessible from outside the controlled area shall result in tamper detection if manipulation of the internal elements can cause an access granted condition. The tamper detection shall occur before the tamper mechanism can be defeated	OP	M	M	M
6	Devices intended to be installed outside the controlled area or that could be accessible from outside the controlled area shall detect removal from mounting if that provides access to the internal elements and manipulation of these elements can cause an access granted condition	OP	OP	M	M
7	The enclosures of the EACS components accessible from outside the controlled area shall meet the required IP and IK ratings	IP4X IK04	IP4X IK04	IP4X IK04	IP4X IK04
8	In case of loss of communication between the control unit(s) and the monitoring console, the control unit should be capable of storing and subsequently transmitting upon restoration of communications a minimum number of events per portal	N/A	OP	500	1000
9	Communication between control unit and the EACS components shall be monitored. The loss of the communication for the indicated duration shall result in an alert at the monitoring console	N/A	OP	10 min	2 min
10	System administration including configuration shall only be logically accessed with the use of valid credentials (e.g. password, token)	N/A	M	M	M
11	There shall be separate access levels that categorize the ability of the operators to perform different functions in the system. Minimum number of logical access levels is:	1	1	2	4
12	The minimum number of required characters for logical access by memorized information only shall be as indicated (N=numeric/A=alphanumeric)	4N	5N	6A	8A
13	If numeric codes are used for logical access by memorized information, sequential ascending or descending pass-code digits and use of same digit more than twice shall not be allowed	OP	OP	M	M

Table 7 (2 of 2)

System self-protection requirements		Grade assignment			
		1	2	3	4
14	Use of minimum 4-digit memorized information for logical access when combined with token or biometrics (to be system generated or by system administrator)	OP	OP	M	M
15	Logical access credential can only be assigned by the system administrator	OP	OP	M	M
16	Manufacturer's pre-set values for logical access shall be capable of being overwritten	OP	OP	M	M
17	After operational power loss minimum data retention time for logged events stored on the access control unit (due to loss of communication with monitoring console) shall be as indicated	OP	24 h	120 h	120 h
18	Encryption required for communication signals between components of the EACS when using publicly shared networks (e.g. the Internet)	OP	OP	M	M
19	The information stored on the token shall be protected against unauthorized modification or reproduction	OP	OP	M	M
20	Either failure or restoration of the communication channel shall not result in the release of an access point	M	M	M	M
21	Failure of communication with monitoring console shall not interrupt the access decision process	M	M	M	M
22	Processing rules stored in an access point reader shall not be visible to system users	M	M	M	M
23	Light or sound keystroke keypad activation indicators shall not be a direct representation of actual codes, but shall be identical in pitch and duration	M	M	M	M
24	Communication between readers and access control units shall support encryption with authentication	OP	OP	OP*	M
25	The instruction manual shall contain details of the installation requirements for the mechanical protection limiting access to the communication lines between readers and access control unit	OP	OP	OP*	OP
B – Detection and reporting					
26	The change in state (open, closed, tamper (open tamper or closed tamper)) of a digital input detection circuit shall be designed by the manufacturer to ensure that the tolerance for each circuit input state shall not overlap an adjacent state	OP	OP	M	M
27	Data entry system validation. System shall provide annunciation when invalid data has been entered during configuration mode at the monitoring console	M	M	M	M
28	Access to the configuration mode shall time out after a pre-set period of inactivity	M	M	M	M
NOTE Abbreviations used in the table are the following: NP = not permitted OP = optional M = mandatory OP* = one of the options in the identified grouping (gray area) shall be implemented N/A = not applicable					

6.9 Power supply requirements

The access control unit and the components of the electronic access control system may be powered either by an integrated or a separate power supply that meets the following requirements and the appropriate requirements in Table 8 for each grade:

- 1) The power supply shall be capable of supporting the electronic access control system in all conditions including recharging of the standby power source within the period specified in Table 8.
- 2) The power supply may be placed in one or more components of the electronic access control system or in a separate housing.

Table 8 – Power supply requirements

Power supply requirements		Grade assignment			
		1	2	3	4
1	The access control unit shall be provided with standby power source capable of operating the unit and its accessories under specified full load condition for the period of time indicated. (The loading conditions do not include the monitoring console or access point actuators)	OP	OP	2 h	4 h
2	Following an extended primary power source failure (system shutdown occurred) and restoration of power, rechargeable batteries shall be recharged to 80 % of rated capacity within 24 hours and 100 % of rated capacity within 72 hours	M	M	M	M
3	Either loss of primary power source or restoration shall not adversely affect the normal operation of the system	OP	OP	M	M
4	If standby power source is provided provisions shall be made to monitor for the following conditions: low voltage level and no battery present (single common annunciation for both conditions is acceptable)	OP	OP	M	M
NOTE Abbreviations used in the table are the following: OP = optional M = mandatory					

7 Environmental and EMC (immunity) requirements

Each component of an electronic access control system is expected to operate correctly in its service environment and to continue to do so for a reasonable time. Access control system equipment is however installed in many very different environments and it would be impractical to test every aspect of the most extreme conceivable environmental conditions and immunity to electromagnetic effects.

The tests and severities identified by this standard are therefore intended to provide a practical series of tests to determine the ability of the equipment to withstand the failure mechanisms most likely to be produced by the environment, in which that type of equipment can be expected to be installed, i.e. the normal service environment.

The applicable environmental conditioning specified in Table 9 shall be conducted in accordance with the methods described in IEC 62599-1.

The applicable electromagnetic compatibility conditioning specified in Table 9 shall be conducted in accordance with the methods described in IEC 62599-2.

Table 9 – Environmental and EMC (immunity) requirements (1 of 2)

Reduced functional test (8.2)		Test	Type	Environmental class I	Environmental class II	Environmental class III	Environmental class IV
1	B,D,A	Dry heat	Operational	M	M	M	M
2	B,A	Dry heat	Endurance	N/A	N/A	N/A	M
3	B,D,A	Cold	Operational	M	M	M	M
4	B,D,A	Damp heat, steady state	Operational	M	N/A	N/A	N/A
5	B,A	Damp heat, steady state	Endurance	M	M	M	M
6	B,D,A	Temperature change (p)	Operational	M	M	M	M
7	B,D,A	Damp heat, cyclic	Operational	N/A	M	M	M
8	B,A	Damp heat, cyclic	Endurance	N/A	N/A	M	M
9	B,C,A	Water ingress	Operational	M(p)	M(p)	M	M
10	B,A	Sulphur dioxide (SO ₂)	Endurance	N/A	N/A	M	M
11	B,A	Salt mist, cyclic	Endurance	N/A	N/A	N/A	M
12	B,C,A	Impact (f) (m)	Operational	M	M	M	M
13	B,A	Dust	Endurance	N/A	N/A	M	M
14	B,C,A	Free fall (m) (p)	Operational	M	M	M	M
15	B,C,A	Shock(f)	Operational	M	M	M	M
16	B,C,A	Vibration, sinusoidal	Operational	M	M	M	M
17	B,C,A	Mains supply voltage variations	Operational	M	M	M	M
18	B,C,A	Mains supply voltage dips and short interruptions	Operational	M	M	M	M
19	B,C,A	Electrostatic discharge	Operational	M	M	M	M
20	B,C,A	Radiated electromagnetic fields	Operational	M	M	M	M
21	B,C,A	Conducted disturbances induced by electromagnetic fields	Operational	M	M	M	M
22	B,C,A	Fast transient bursts	Operational	M	M	M	M
23	B,C,A	Slow high energy voltage surge	Operational	M	M	M	M