IEC 60839-11-1

Edition 1.0 2013-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC 60839-11-1:2013

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It also gives information on projects, replaced and withdrawn publications.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

IEC 60839-11-1

Edition 1.0 2013-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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 60839-11-2[1]. 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