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It also gives information on projects, replaced and withdrawn publications.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

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

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.

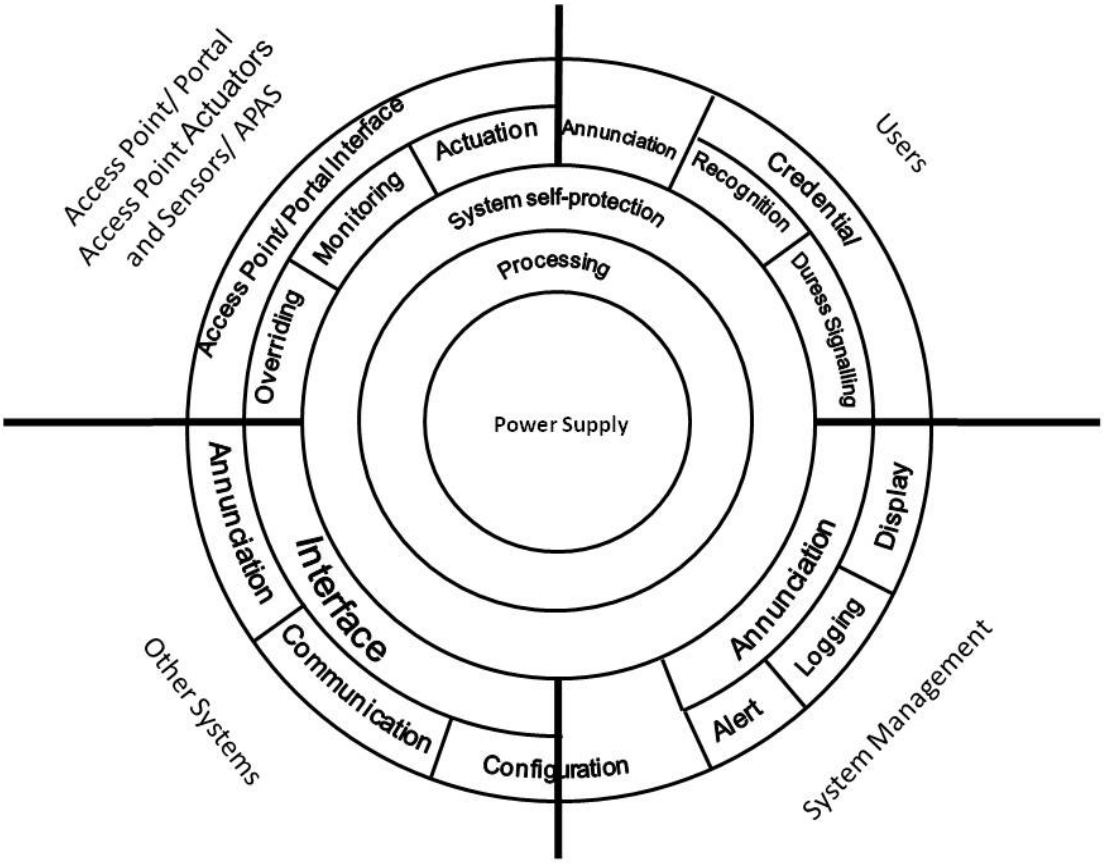
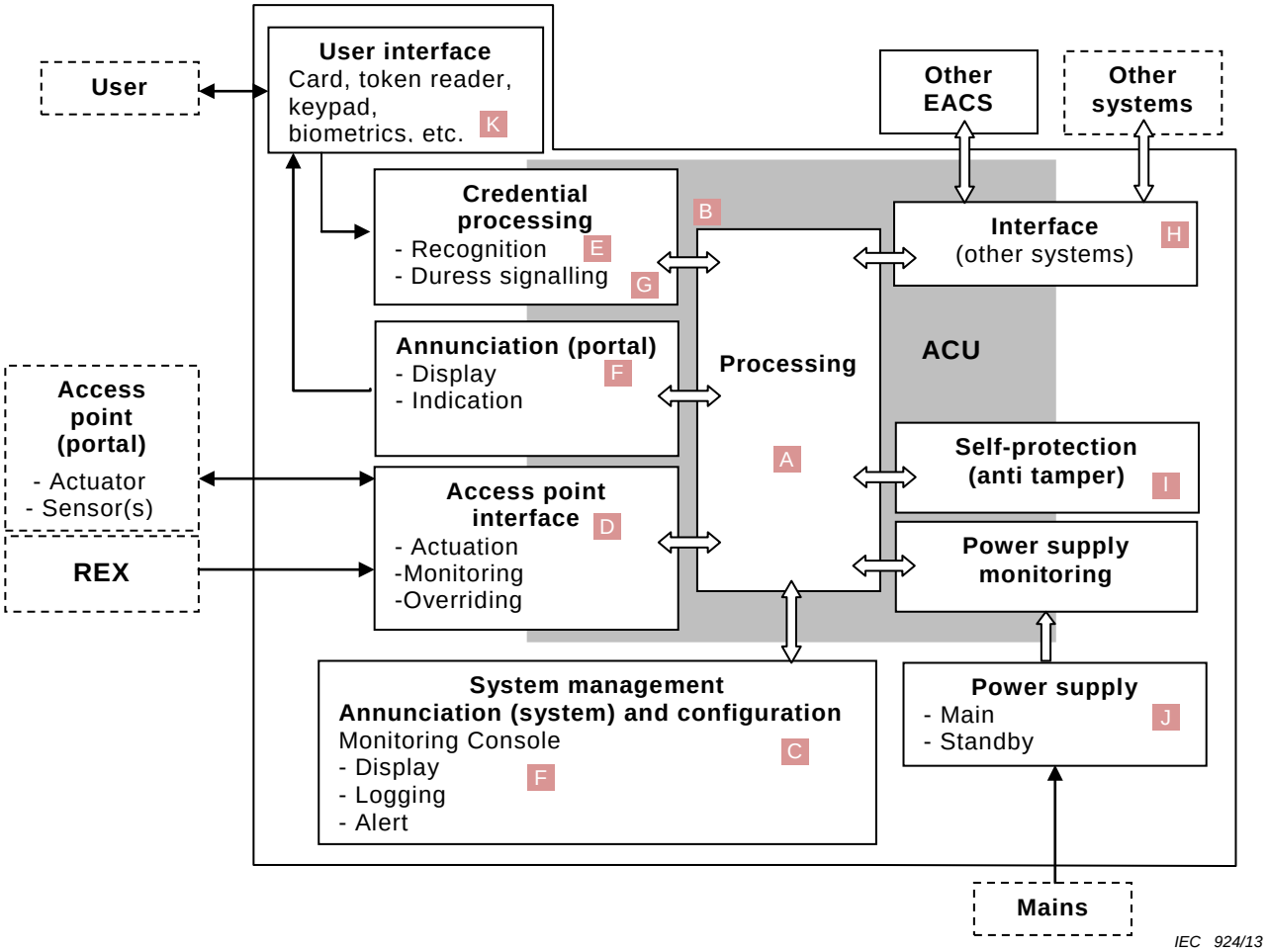


Figure 1 – Conceptual model *IEC 923/13*



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 $FAR_{\text{eff}} = FAR$ (false acceptance rate) when 1:1 comparison is performed (e.g. biometric verification of an identity claimed by memorized information or token) or $FAR_{\text{eff}} = FAR \times n$ 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 ($S0_2$)	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

Table 9 *(2 of 2)*

Note Abbreviations used in the table are the following:	
A	after conditioning and recovery period
B	before conditioning
C	monitor during conditioning
D	during conditioning, monitor and conduct reduced functional test as specified in IEC 62599-1
M	mandatory
N/A	not applicable
(f)	applicable to fixed equipment
(m)	applicable to moveable equipment
(p)	applicable to portable equipment

8 Test methods

8.1 General conditions

8.1.1 Atmospheric conditions for tests

Unless otherwise stated in a test procedure, the testing shall be carried out after the test specimen has been allowed to stabilize in the standard atmospheric conditions for testing as described in IEC 60068-1 as follows:

– temperature: (15 to 35) °C;

– relative humidity: (25 to 75) %;

– air pressure: (86 to 106) kPa.

If variations in these parameters have a significant effect on a measurement, then such variations should be kept to a minimum during a series of measurements carried out as part of one test on one specimen.

8.1.2 Operating conditions for tests

If a test method requires a specimen to be operational, then the specimen shall be connected to power supply equipment set within the manufacturer's specified voltage range(s) and shall remain substantially constant throughout the tests. If a test procedure requires a specimen to be monitored to detect any alert signals, then connections shall be made to any necessary ancillary devices to allow the signal to be recognized.

All input signals/messages shall be correctly terminated according to the manufacturer's instructions.

Outputs shall be connected to loads representative of maximum conditions within the manufacturer's specification.

All transmission paths shall be connected to compatible equipment. All output circuits shall be connected to maximum loads, all within the manufacturer's specification.

8.1.3 Specimen configuration

The specimen configuration shall include at least one of each type of compatible/supported access point user interfaces, access point actuators or equivalent indicators (with equivalent loads), monitoring console application or equivalent (if provided), configured by the manufacturer to provide the grade dependent operation as defined in Table 2 through Table 8.

Any additional equipment necessary to carry out the tests (for example: means to monitor the status of outputs and means to activate inputs) shall be supplied by the manufacturer by agreement with the test house.

The specimens submitted shall be representative of the manufacturer's normal production with regard to their construction and configuration settings and shall include the claimed options.

8.1.4 Mounting arrangements

The specimen shall be mounted by its normal means of attachment in accordance with the manufacturer's instructions. If these instructions describe more than one method of mounting then the method considered to be the least favourable shall be chosen for each test.

8.1.5 Tolerances

Unless otherwise stated, the tolerances for the environmental test parameters shall be as given in the basic reference standards for the test (e.g. the relevant part of IEC 60068). If a specific tolerance or deviation limit is not specified in a requirement or test procedure, then a deviation limit of ± 5 % shall be applied.

8.1.6 Provisions for tests

At least one access control system shall be provided for testing compliance with this part of IEC 60839. The specimens submitted shall be representative of the manufacturer's normal production with regard to their construction and settings and shall include the claimed options.

The requirements listed in 6.2 to 6.9 shall be tested using the access control system/ components connected in accordance with the example system defined in Figure 3 (or part of it as deemed applicable) and having the functions configured by the manufacturer to provide the grade dependent operation as defined in Table 2 to Table 8.

Where individual components are assessed to this standard, e.g. a reader, the tests shall be performed with that component connected to an access control system configured at a minimum to support the operation of that component. Alternatively, it is permitted to test individual components by simulating the functions of an access control system provided there is agreement between the applicant and the test authority that the method of simulation is appropriate to verify applicable functionality for the respective component.

Components of EACS carrying several functionalities described in Clause 6 shall be assessed by selecting the relevant tests described in Clause 8 for the appropriate grade. It is the responsibility of the test house to make this selection in accordance with the functionalities and grade rating claimed by the manufacturer.

8.1.7 Optional functions

This part of IEC 60839 specifies mandatory and optional functionalities. An access control unit or component of an access control system complying with this part of IEC 60839will need to fulfil the requirements of all of the mandatory functions.

If a function is provided that is optional for a particular grade and a claim of compliance is made, it shall meet the applicable requirements for the grade for which compliance is claimed and it shall be tested.

Functionalities additional to the mandatory ones specified in this standard may be included in the electronic access control system providing they do not prevent the correct operation of the mandatory functionalities.

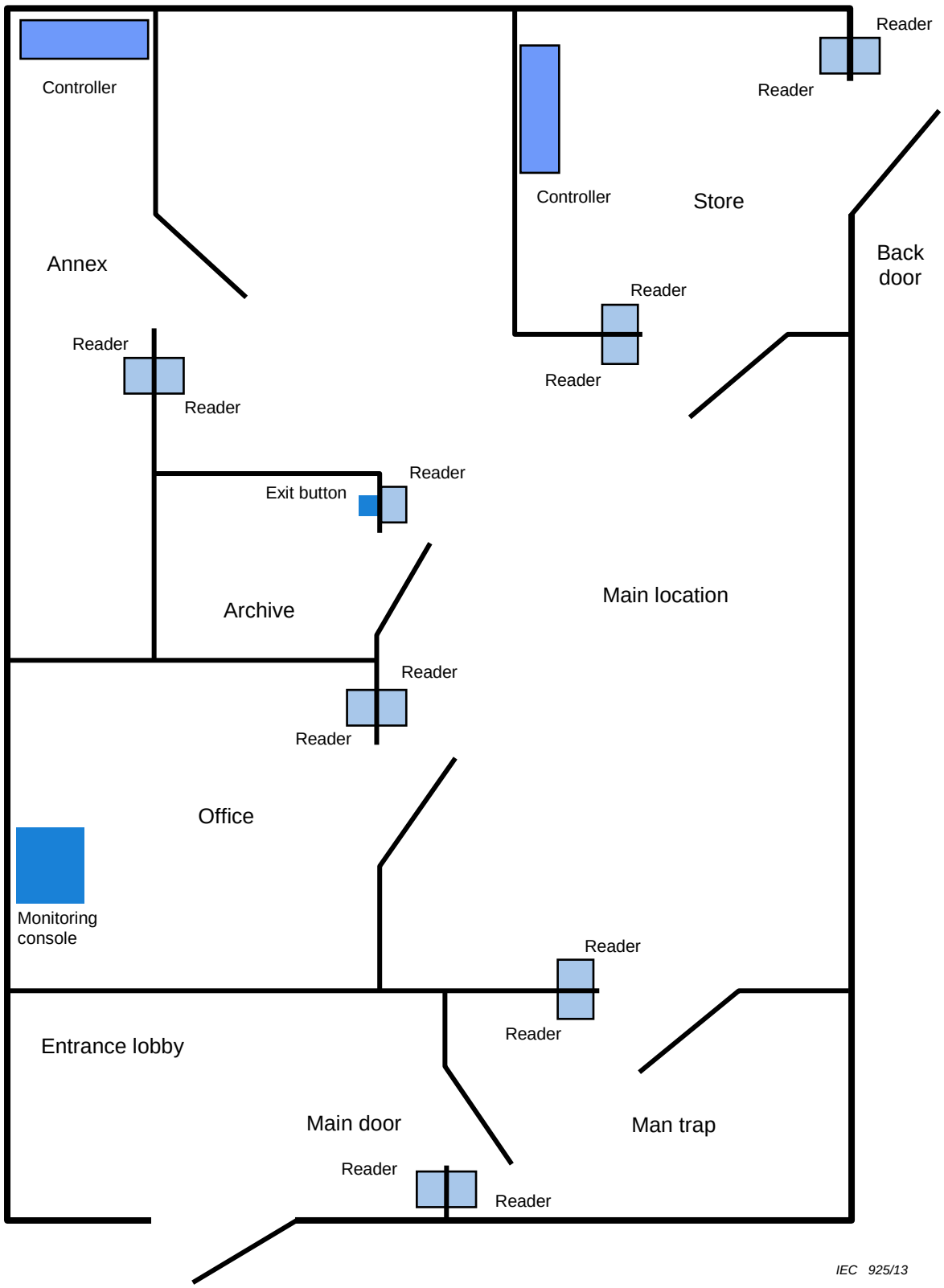


Figure 3 – Example of system test configuration

8.2 Reduced functional test

For specified tests, (for example: environmental tests, EMC tests), it may not be possible or desirable to carry out a full functional test. In these cases a reduced functional test shall be carried out in accordance with the procedure below:

1) Present valid credentials to an access point to create an access granted condition and simulate the portal being opened and closed.
2) Record the response of the annunciation outputs at the access point and confirm the functionality is as per Table 3, line 1.
3) Confirm by inspection that an indication of access point locked status is displayed until an access is granted and functionality is as per Table 3, line 3.
4) Present invalid credentials to an access point to create an access denied condition and record the response of the annunciation outputs and check that the cause of access denial is placed in the event log.
5) Confirm the functionality is as per Table 3, lines 2, 17 and 18.
6) Present valid credentials to an access point to create an access granted condition and simulate the portal being opened. Keep the portal open until after the allowed open expiry time and confirm an alert is generated.
7) Confirm the functionality is as per Table 3, lines 4 and 32.
8) Close the portal and confirm the functionality is as per Table 3, lines 4 and 26.

8.3 Functional tests for access point interface

8.3.1 Object of the test

To demonstrate the ability of the access control unit to comply with the requirements in 6.2 and Table 2.

8.3.2 Principle

The access control system of Figure 3 shall be operated to demonstrate the security classification dependent functions as listed in the requirements of Table 2. Using the programmed credentials (codes, cards, etc.), present them to the access point, monitor that the input has been processed within the required time period and that the correct indication and notification(s) occur (see Table 2). The laboratory shall check the manufacturer's documentation for the support of mandatory and optional functionalities described in Table 2 for the grade that is assigned to the access control unit.

8.3.3 Procedure

8.3.3.1 Access point interface – Release timing (ref. Table 2, lines 1 to 4)

To demonstrate the ability of the access control unit to comply with requirements in Table 2, lines 1 to 4, perform the following steps:

1) The system shall be programmed for one valid user information (credential), and in normal condition.
2) Verify the manufacturer's documentation and determine whether the release time is system defined or configurable for each access point (portal).
3) Enter the user information, access shall be granted.
4) Measure the release time and record result, functionality shall be as per Table 2, lines 1 to 4.

8.3.3.2 Access point interface – Access control (ref. Table 2, lines 5 to 19)

To demonstrate the ability of the access control unit to comply with requirements in Table 2, lines 5 to 19, perform the following steps:

1) The system shall be programmed for one valid user information (credential) and in normal condition. The system shall be provided with two access points, one programmed as entry and another one programmed as exit from a controlled area.
2) Verify the manufacturer's documentation and determine if the anti-passback rule is implemented and what options of this rule are supported (hard, soft, timed, global, override/disable, and anti-passback times). Enable one supported anti-passback function at the time.
3) Enter the user information at the entry access point and verify that access is granted. Functionality shall be as per Table 2, line 5.
4) Enter the same user information again at the entry access point (before and after the programmed anti-passback time) and record the result.
5) Enter the user information at the exit access point and verify that access is granted. Functionality shall be as per Table 2, line 6.
6) Enter the same user information again at the exit access point (before and after the programmed anti-passback time) and record the result.
7) Repeat the test for each anti-passback option supported by the access control system.
8) Functionality for supported anti-passback options shall be as per Table 2, lines 7 to 11.
9) Program an effective date/expiry date for the user information.
10) Enter the user information at the access point within the effective date/before expiry date set for this credential, access shall be granted.
11) Enter the user information at the access point after the effective date/expiry date set for this credential, access shall be denied. Functionality shall be as per Table 2, lines 12 and 13.
12) Program two users information with the same access levels.
13) Program an access point to allow entry only when two sequential authorized access requests are made within a programmable limited time period. Program allowed window to 2 minutes.
14) Present one user information, access shall not be granted.
15) Present the first and second user information within 2 minutes, access shall be granted
16) Present the first user information, wait for 2 minutes, present the second user information, access shall not be granted. Functionality shall be as per Table 2, line 17.

8.3.3.3 Access point interface – Access point status monitoring (ref. Table 2, lines 20 to 23)

To demonstrate the ability of the access control unit to comply with requirements in Table 2, lines 20 to 23, perform the following steps:

1) The system shall be programmed for one valid user information (credential), and in normal condition.
2) Verify the manufacturer's documentation and determine whether the access point open time is system defined, programmable for each access point/portal.
3) Enter the user information, access shall be granted.
4) Measure the open time of the portal and record the result. Functionality shall be as per Table 2, lines 20 to 22.

8.3.3.4 Access point interface – Input signals processing (ref. Table 2, line 24)

Apply an input signal (e.g. tamper) with an active duration of minimum 400 ms and record whether the event is annunciated at the monitoring console. Functionality shall be as per Table 2, line 24.

8.3.4 Criteria for compliance

The status of the access point actuation and monitoring shall be in accordance with the security classification dependent requirements of Table 2.

8.4 Functional tests for indication/annunciation (displaying, alert and logging)

8.4.1 Object of the test

To demonstrate by inspection and test that the access control system can meet the indication/annunciation functionalities of 6.3 and Table 3.

8.4.2 Principles

The access control system of Figure 3 shall be operated to demonstrate the security classification dependent functions of display, alert and logging functions as listed in the requirements of Table 3.

8.4.3 Test procedure

8.4.3.1 Portal indications (ref. Table 3, lines 1 to 4) and monitoring console annunciation (ref. Table 3, lines 17, 18, 26 and 32)

To demonstrate the ability of the access control unit to comply with requirements in Table 3 lines 17, 18, 26 and 32 perform the following steps:

1) Where the option is provided verify that an indication of portal locked status is displayed until an access is granted. Functionality shall be as per Table 3, line 3.
2) Present valid credentials to an access point to create an access granted condition. Record the response of the annunciation outputs at the portal. Functionality shall be as per Table 3, line 1.
3) Present invalid credentials to an access point to create an access denied condition and record the response of the annunciation outputs. Ensure that the cause of access denial is placed in the event log. Functionality shall be as per Table 3, lines 2 and 18.
4) For system defined operation, present valid credentials to an access point to create an access granted condition and simulate the portal being open. Keep the portal open until the system defined pre-alert time starts and record the response of the annunciation outputs at the portal. Keep the portal further open until the system-defined allowed open time expired and confirm an alert is generated at the monitoring console. Functionality shall be as per Table 3, lines 4 and 32.
5) Close the portal and record the time taken for the alert to cease. Functionality shall be as per Table 3, lines 4 and 26.

8.4.3.2 Monitoring console (Ref. Table 3, lines 5 to 47)

To demonstrate the ability of the access control unit to comply with requirements in Table 3, lines 5 to 47, perform the following steps:

1) Present valid credentials to an access point to create an access granted condition and simulate the portal being opened and closed. Record the response of the annunciation outputs at the monitoring console. Functionality shall be as per Table 3, lines 6, 15 and 27.
2) Where the option is provided, confirm there is visual annunciation when access is granted. Functionality shall be as per Table 3, line 5.
3) Where the option is provided, check the operation of the card usage counter annunciation. Functionality shall be as per Table 3, line 8.
4) Create a duress condition and record the response of the annunciation outputs at the monitoring console. Functionality shall be as per Table 3, line 7.

5) Present a token with an expired validity period to an access point and record the response of the annunciation outputs. Functionality shall be as per Table 3, line 9.

6) Present a valid token together with valid memorized information (e.g. PIN) to a suitably configured access point to create an access granted condition and simulate the portal being opened and closed. Confirm correct operation as per Table 3, lines 1, 6, 15 and 27.

7) Repeatedly present a valid token together with invalid memorized information (e.g. wrong PIN) at the same portal. Monitor the response of the annunciation outputs and record the number of attempts until an alert indication is given. Functionality shall be as per Table 3, line 10.

8) Present valid memorized information (e.g. PIN) to a suitably configured access point to create an access granted condition and simulate the portal being opened and closed. Confirm correct operation as per Table 3, lines 1, 6, 15 and 27.

9) Repeatedly present invalid memorized information (e.g. wrong PIN) at the same portal. Monitor the response of the annunciation outputs and record the number of attempts until an alert indication is given. Functionality shall be as per Table 3, line 11.

10) Subject to security classification, confirm by inspection that the system has provision to display a map of the controlled area and access points for which an alert was generated. Functionality shall be as per Table 3, line 13.

11) Subject to security classification, confirm by inspection that the system has provision to display instructions following an alert condition. Functionality shall be as per Table 3, line 12.

12) Commencing with the simulated portal closed, present valid credentials to an access point to create an access granted condition but keep the portal closed, simulating a failure to entry condition. Record the response of the annunciation outputs at the portal and confirm the uncompleted transaction is recorded in the event log and an alert indication is provided as per Table 3, line 16.

13) Confirm by test that changes to time scheduled and/or manual (via manual override release) portal locked/unlocked status are displayed and the event is recorded in the log. Functionality shall be as per Table 3, line19.

14) Remove the primary power source (e.g. mains supply) to the system under test. Record the response of the annunciation outputs. Functionality shall be as per Table 3, lines 20, 27 and 28.

15) Reinstate the primary power source and confirm the event is recorded in the log. Functionality shall be as per Table 3, line 21.

16) Create a condition of low standby power supply by either introducing a discharged battery or by substituting the normal standby power source with a variable power supply adjusted slowly from the nominal standby voltage to the low power condition. Record the response of the annunciation outputs when the low power condition is reached. Functionality shall be as per Table 3, lines 22, 27 and 28.

17) With the normal standby power supply reinstated and the access control system functioning normally completely remove the standby power source. Record the response of the annunciation outputs. Functionality shall be as per Table 3, lines 22, 27 and 28.

18) Confirm by test that the action of entering and the action of leaving the programming mode is displayed and is recorded in the event log. Functionality shall be as per Table 3, line 23.

19) Interrupt the following communication links in turn whilst monitoring the annunciation outputs and measuring the time taken for the alert to be annunciated:

    a) the link between the access point user interface and the access control unit;

    b) the link between the access control unit and the monitoring console.

20) Upon the interruption of the link between the access point user interface and the access control unit, measure and record the duration from the moment of interruption to the moment the alert is indicated at the monitoring console. Functionality shall be as per Table, 3 lines 24, 27, 28, 35 and 38.

21) Where the option of displaying text instructions is provided following an alert, also measure and record the duration from the moment that the alert is indicated at the monitoring console to the moment that the text instructions associated with the alert message are displayed at the monitoring console. Functionality shall be as per Table 3, line 39.

22) Where the option of displaying images and/or graphics is provided following an alert, also measure and record the duration from the moment that the alert is indicated at the monitoring console to the moment that the images and/or graphics associated with the alert message are displayed at the monitoring console. Functionality shall be as per Table 3, line 40.

23) Create system alerts at items that are off-line. Note the time and wait at least 5 minutes.

24) Each communication link shall be reinstated and correct operation shall be demonstrated between the interruption attempts. Functionality shall be as per Table 3, lines 14 and 27.

25) Check that the system alerts are received in the log with date stamps of the time the alert occurred, not the time it was received at the monitoring console. Functionality shall be as per Table 3, line 27.

26) Present five sets of valid credentials to one or more access points in turn, creating an access granted condition and simulating the portal being opened and closed each time. Then remove one set of credentials from the controlled area by implementing an appropriate exit procedure.

27) Monitor and record the response of the annunciation outputs and confirm that:

    a) the event log roll call reflects the correct number of credentials recorded as still being “IN” the area controlled by the system. Functionality shall be as per Table 3, line 25;

    b) the credentials that were removed from the controlled area by implementation of the exit procedure are correctly identified as being outside the controlled area;

    c) the event log shall have recorded the identity of specific reader(s) to which the credentials were presented.

28) With the access control system operating normally and with all portals in a secured condition apply the appropriate inputs to simulate the action of a forced opening, i.e. without access being granted. Record the response of the annunciation outputs. Functionality shall be as per Table 3, line 31.

29) Open an enclosure fitted with a means to detect tampering and record the response of the annunciation outputs. Functionality shall be as per Table 3, line 30.

30) Simulate a locking device abnormal condition by application of the appropriate input signal(s) and record the response of the annunciation outputs. Functionality shall be as per Table 3, line 36.

31) With reference to the manufacturer's documentation create a sufficient number of events to fill the event log to 90 % of logging capacity. Functionality shall be as per Table 3, line 37.

32) Confirm by test that priorities can be assigned to specific alert events. Select at random, at least three configurable alert events. Functionality shall be as per Table 3, lines 28, 29 and 41.

33) Generate multiple (minimum three) configurable alert events that have assigned specific priorities. Record the response of the annunciation outputs. Acknowledge each alert event and again record the response of the annunciation. Confirm that alerts were displayed in the order of priorities as specified by the access control manufacturer. Functionality shall be as per Table 3, line 29.

34) Exercise the access control system to generate one of the selected alert events. Record the response of the annunciation outputs. Acknowledge the alert event and again record the response of the annunciation outputs. Functionality shall be as per Table 3, line 42.

35) Where the option is provided for the operator to include comments in response to alerts, confirm also that the system generates an entry in the event log. The entry shall include a

time and date stamp, the alert event to which the comments relate and the identity of the operator. Functionality shall be as per Table 3, line 45.

36) Present five sets of valid credentials to one or more access points in turn, creating an access granted condition and simulating the portal being opened and closed each time. Then remove four sets of credentials from the controlled area by implementing the appropriate exit procedures. Monitor and record the response of the annunciation output and confirm that a warning associated with the minimum number of persons not present is displayed together with an alert and an entry in the event log. Functionality shall be as per Table 3, line 43.

37) Confirm by test that operator initiated changes are recorded in the event log. Functionality shall be as per Table 3, line 44.The record shall include the following:

    a) type of parameter changed;

    b) operator identification;

    c) time and date stamp.

38) Creation, printing and exporting of management reports shall be checked against the manufacturer's specification. Functionality shall be as per Table 3, line 46.

    At minimum, reporting for Grade 3 and Grade 4 systems shall include:

    a) details of all circuit activities;

    b) summary of all or any selected circuit activity including individual alarms within a chosen time period. (E.g. the system shall be capable of searching for all circuit activity or a single circuit within for example the last hour, even if there have been no alarm events);

    c) circuit and reader related operator actions within a chosen time period;

    d) access control alarms;

    e) access control reader activity on a per user basis;

    f) access control user information;

    g) circuit information: full point detail for every configured input and output point;

    h) user database changes;

    i) system availability: a log of all parts of the system, which details periods when each individual part is on-line and off-line;

    j) database files and system configurations.

39) By inspection of the manufacturer's documentation confirm that the monitoring console has the provision to meet the security classification dependent requirements for the minimum event logging capacity of the system. Functionality shall be as per Table 3, line 47.

40) Present three valid credentials at three different readers. Functionality shall be as per Table 3, line 33.

41) Present three different valid credentials at one reader and two non-valid credentials at the same reader. Functionality shall be as per Table 3, line 34.

8.4.4 Criteria for compliance

The status of the annunciation outputs shall be in accordance with the security classification dependent requirements of Table 3.

8.5 Test methods for recognition functionalities

8.5.1 Object of the test

To demonstrate by inspection and test that the access control system can meet the recognition functionalities of 6.4 and Table 4.

8.5.2 Principles

The access control system of Figure 3 shall be operated to demonstrate the security classification dependent functions of recognition operate as listed in the requirements of Table 4.

8.5.3 Test procedure

8.5.3.1 Access levels (ref. Table 4, lines 1 to 12)

To demonstrate the ability of the access control unit to comply with requirements in Table 4 lines 1 to 12, perform the following steps:

1) At the beginning of all tests set the real time clock to the correct time. After one day check whether the real time clock differs from the correct time by not more than the allowed value calculated as per Table 4, line 1.
2) Set the date to date of change from the normal time to daylight saving time and the time to 2 minutes before the expected change. Record whether the change from the normal time to daylight saving time occurs at the official changing time as per Table 4, line 1.
3) Set the date to date of change from daylight saving time to the normal time and time to 2 minutes before the expected change. Record whether the change from daylight saving time to normal time occurs at the official changing time as per Table 4, line 1.
4) Set the date to February 28th of a next leap year and the time to 23:58. Record whether at midnight the date changes to February 29th as per Table 4, line 1.
5) Set the date to February 28th of a non-leap year and the time to 23:58. Record whether at midnight the date changes to March 1st as per Table 4, line 1.
6) Set the master clock to the correct time and date. Set the slave real time clock to the wrong time and wrong date. Set the time of the master clock to 2 min before synchronization time (given by the manufacturer). Record whether after the synchronization time the slave real time clock is synchronized to the same date and time as the master clock. By reviewing the accompanying documentation confirm that the synchronization time is repeated every day (i.e. with no input of date). Functionality shall be as per Table 4, line 3.
7) Set master clock of the access control unit to the wrong time and wrong date. Connect the master clock of EACS to the official master clock of the premises, which gives the official time. After a maximum period of 15 minutes confirm that the master clock of the EACS has synchronized to the official time as per Table 4, line 4.
8) Confirm the real time clock is set to display the correct time. Disconnect the mains power supply and the standby batteries (data retention batteries shall remain connected). After the periods defined by the appropriate system grade, reconnect the mains power supply and the standby batteries. The order of reconnection shall be in accordance with the equipment manufacturer's recommendations. Confirm by inspection of the real time clock that the access control system displays the correct time. Functionality shall be as per Table 4, line 5.
9) Review the manufacturer's documentation and determine that the number of user access levels and the number of time zones meet or exceed the requirements of Table 4, lines 6 and 7.
10) Verify whether the input of day, week, hour and minute, or the date, year, month and day, or hour and minute, respectively, is possible for the access levels required by Table 4, lines 8 and 9.
11) Verify whether the given number of configurable days (i.e. special days) is handled correctly by the electronic access control system as per Table 4, line 10.

8.5.3.2 Equipment and methods of recognition (ref. Table 4, lines 13 to 27)

To demonstrate the ability of the access control unit to comply with requirements in Table 4, lines 13 to 27, perform the following steps:

1) Attempt to add a new token to the system with the same number of already authorized tokens or attempt to assign the same token to two users. Confirm the attempt is rejected. Functionality shall be as per Table 4, line 13.
2) Set the EACS in operation with no access levels assigned to any user/cardholder. Assign an appropriate credential to a user/cardholder of the system. Assign an access level to this user. Apply the credential to an appropriate reader/keyboard or biometric sensor during a permitted entry period. Confirm whether access is granted. Apply any other credential not known to the system to the reader/keyboard/biometric sensor and confirm that access is denied. Functionality shall be as per Table 4, lines 14 to 17.
3) Verify that each access attempt with a valid token and invalid memorized information is denied. Verify that after the number of attempts stated in Table 4, line 18, this credential is blocked in accordance with the parameter(s) set in the configuration of the system.
4) Review the manufacturer's documentation and confirm the required FAR levels for biometrics devices (when used with the access control unit for the appropriate grade) are indicated. Information shall be as per Table 4, line 20.
5) Review the documentation and verify the number of valid code differs are met for the number of users allowed by the system for each grade. Information shall be as per Table 4, line 21.
6) Review the documentation and verify that the minimum number of digits used for memorized information is as per Table 4, line 22.
7) Assign to 10 users a token with a facility/user code. Enter a new user/cardholder and try to assign to the new user a token which already is used. Confirm that the system refuses this input and gives notice that this token has already been allocated. Functionality shall be as per Table 4, line 24.
8) Assign tokens with different facility codes and the same user code to two or more users. Confirm that the system allows the input of different facility codes. Functionality shall be as per Table 4, line 24.
9) Review the manufacturer's documentation and confirm whether a degraded mode of operation is supported or not. Verify that a degraded mode may be disabled automatically or manually by a supervisor level access, when the system is investigated for Grade 4 functionality. Functionality shall be as per Table 4, line 25.
10) Verify on the tokens intended to be used with the system whether the encoding structure is visible (e.g. transparent token), or whether the complete encoding is printed on the token. Information shall be as per Table 4, lines 26 and 27.

8.5.4 Criteria for compliance

The recognition functionality shall be in accordance with the security classification dependent requirements of 6.4 and Table 4.

8.6 Functional tests for duress signalling

8.6.1 Object of the test

To demonstrate by inspection and test that the duress signalling requirements of 6.5 and Table 5 can be met.

8.6.2 Principles

The duress feature of the access control system described in Figure 3 shall be operated to demonstrate the access control system outputs associated with duress signalling can fulfil the security classification dependent requirements of Table 5.

8.6.3 Test procedure (ref. Table 5, lines 1 to 3)

To demonstrate the ability of the access control unit to comply with requirements in Table 5, lines 1 to 3, perform the following steps:

1) To confirm that duress signalling is configurable follow the manufacturer's instructions to program the duress function. Functionality shall be as per Table 5, line 1.
2) Using the appropriate procedure, provide a duress input. Monitor and record the alert received at the monitoring console. Confirm that the duress alert is distinguishable from other alerts. Functionality shall be as per Table 5, line 2.
3) By test and inspection confirm that the duress initiating device (e.g. reader, keypad) does not produce an audible or visible local indication. Functionality shall be as per Table 5, line 3.

8.6.4 Criteria for compliance

Duress signalling shall be configurable portal by portal and the associated alert outputs shall be in accordance with the security classification dependent requirements of Table 5.

8.7 Functional tests for overriding

8.7.1 Object of the test

To demonstrate by inspection and test that the electronic access control system can meet the overriding functionalities of 6.6 and Table 6.

8.7.2 Principles

The access control system of Figure 3 shall be operated to demonstrate the security classification dependent functions of overriding as listed in the requirements of Table 6.

8.7.3 Test procedure (ref. Table 6, lines 1 to 7)

To demonstrate the ability of the access control unit to comply with requirements in Table 6, lines 1 to 7, perform the following steps:

1) Inspect the manufacturer’s documentation for the overriding process. Set one of the readers to single free access status. Record whether the door is free for one access procedure and then reset to normal access granting process. Functionality shall be as per Table 6, line 1.
2) Review the manufacturer’s documentation and determine that there is a statement that installation and operation of the EACS shall not prevent the functionality of the emergency exit functions. Information shall be as per Table 6, line 5.
3) Inspect the manufacturer’s documentation for support of scheduling portals for timed blocked access. Enter for one of the access points the time and date of beginning and time and date of ending of the blocked access.
4) Set time and date to 2 minutes before the beginning of the blocked access status and verify that access is granted. After the beginning of the blocked access period check whether access is not granted for several access procedures.
5) If supported according to Table 6, line 7, set time and date to 2 minutes before the end of the blocked access status and check whether access is not granted. After end of blocked access period check whether access is granted when normal access granting procedure is performed.

8.7.4 Criteria for compliance

The overriding functionality shall be in accordance with the security classification dependent requirements of 6.6 and Table 6.

8.8 Functional tests for communication and self-protection

8.8.1 Object of the test

To demonstrate by inspection and test that the electronic access control system can meet the self-protection requirements of 6.7, 6.8 and Table 7.

8.8.2 Principles

The access control system of Figure 3 shall be operated to demonstrate the security classification dependent functions of communication and self-protection as listed in the requirements of Table 7.

8.8.3 Test procedure (ref. Table 7, lines 1 to 28)

To demonstrate the ability of the access control unit to comply with requirements in Table 7, lines 1 to 28, perform the following steps:

1) If memory retention component(s) are non-volatile (example: EEPROM) check the data supplied by the manufacturer and verify that storage components are non-volatile for the period required by Table 7, lines 1 and 17.
2) If memory retention components are volatile (example: RAM), record the system configuration settings and stored events before removal of power.
3) Disconnect the mains power supply and the standby batteries (data retention batteries shall remain connected) for the period of time required by Table 7, lines 1 and 17.
4) After the period defined by the appropriate system grade, as per Table 7, lines 1 and 17, reconnect the mains power supply and the standby batteries. The order of reconnection shall be in accordance with the equipment manufacturer's recommendations. Functionality shall be as per Table 7, line 2.
5) By inspection, compare the recorded system configuration settings and stored events with those of the access control system after reinstating power. The settings and the content of the event log shall not be lost or corrupted (with the exception of power failure and restoration events) and the real time clock shall continue to display the correct time.
6) In conjunction with the manufacturer of the access control system, determine a method by which checksum errors or data loss can be introduced or simulated. For example by erasing stored events from non- volatile memory, such that the access control unit cannot restart properly upon re-instatement of power. Functionality shall be as per Table 7, line 3.
7) Review the manufacturer's documentation for reference to the tool(s) required to open the housing of the access control unit or the component of the access control system. Functionality shall be as per Table 7, line 4.
8) Mount the access control system component according to the manufacturer's instructions with the housing securely closed.
9) Open the housing by normal means (using the tools and instructions provided in the manufacturer's instructions) and attempt to introduce a sabotage tool (steel rod as defined in IEC 60529 with 1 mm diameter and 100 mm long) into the unit without causing physical damage and before tamper detection operates.
10) If the tool is successfully inserted it should be manoeuvred to try to interfere with the tamper detection mechanism or other internal components and cause an access granted condition. Functionality shall be as per Table 7, line 5.
11) Position the access control unit or component of the access control system on a horizontal flat surface taking into account any requirements specified by the manufacturer to operate the removal from mounting detection mechanism.
12) Lift the equipment from the flat surface in a perpendicular direction to the mounting surface and attempt to slide a flat bar 10 mm wide, longer than 300 mm and 1 mm thick, to defeat the removal from the mounting detection. Functionality shall be as per Table 7, line 6.

13) Review the manufacturer's documentation for reference to the appropriate IP and IK rating. Information shall be as per Table 7, line 7.

14) Disconnect the communication channel between the access control unit and the monitoring console. While communication with the monitoring console is interrupted generate access requests using valid credentials and verify functionality is as per 6.7, item 3) and Table 7, lines 8, 20 and 21.

15) Restore communication with the monitoring console. Functionality shall be as per Table 7, line 8.

16) Review the manufacturer's documentation to verify the number of stored events capability in the access control unit while the communication with the monitoring console is lost. Functionality shall be as per Table 7, line 8.

17) With the access control system operating normally as per Figure 3, disconnect the communication circuit between the access control unit and an access point interface (reader) for the duration indicated in Table 7, line 9. Repeat the test as appropriate for other types of communication circuits supported by the access control unit. Functionality shall be as per 6.7, item 4) and Table 7, lines 9, 18, 19 and 20.

18) Review the manufacturer's documentation and confirm implementation of the requirements as per Table 7, lines 24 and 25.

19) Review the manufacturer's documentation and confirm that tokens accepted by the access control system and their initialization procedure comply with the security grade requirements as per 6.8, item 9) and Table 7, line 19.

20) Review the manufacturer's documentation and confirm that access to the configuration of the access control unit is restricted by the use of valid credentials (defined in accordance with the security grade claimed) and that it is possible to restrict access to different functions in the system by access levels. Functionality shall be as per Table 7, lines 10 to 16.

21) Verify that processing rules stored in access point readers (e.g. via dip switches) are not visible from outside the reader enclosure when the reader is installed. Compliance shall be as per Table 7, line 22.

22) Confirm by pressing each keypad button that the audible sound (if available) is identical for all keys. Functionality shall be as per Table 7, line 23.

23) With the access control system in configuration mode, attempt to enter from the monitoring console invalid data (for example other than a supported format or type of characters expected) and confirm data is not accepted by the system. Functionality shall be as per Table 7, line 27.

24) Access the configuration mode at the monitoring console and do not enter any data. Monitor the effect of the inactivity period on the system. Functionality shall be as per Table 7, line 28.

8.8.4 Criteria for compliance

The communication and self-protection functionalities shall be in accordance with the security classification dependent requirements of 6.7, 6.8 and Table 7.

8.9 Power supply requirements

8.9.1 Test of standby power duration

8.9.1.1 Object of the test

The standby power requirements of Table 8, line 1, shall be demonstrated by tests and inspection in accordance with the following procedure.

8.9.1.2 Test procedure

To demonstrate the ability of the power supplies used with the electronic access control system to comply with requirements in Table 8, line 1, perform the following steps:

1) Connect to the access control system (excluding the monitoring console and access point actuators) a power supply with the standby batteries of the type and capacity recommended by the manufacturer. Outputs of the components shall be connected to loads representative of maximum conditions (I_{max}) within the manufacturer's specification.
2) The access control system and accessories shall be monitored throughout the test to identify any changes of state.
3) Charge the batteries for a minimum duration of 24 h while the power supply is connected to the nominal mains supply (V_n).
4) Confirm correct operation by application of the reduced functional test.
5) Disconnect the mains power source and confirm there is no unintentional change of state.
6) Allow the access control system and accessories to operate from the standby batteries for the duration defined by the appropriate system grade of Table 8.
7) Immediately after operating on standby batteries for the required duration, confirm correct operation of the access control unit and accessories by application of the reduced functional test.
8) Reconnect the mains power source and again confirm there is no unintentional change of state.

8.9.1.3 Criteria for compliance

The requirements of the reduced functional test shall be met following the period of operation on the standby batteries and there shall have been no unintentional changes of state.

8.9.2 Test of charger and standby power source capacity

8.9.2.1 Object of the test

The recharging capability requirements of Table 8, line 2, shall be demonstrated by tests and inspection in accordance with the following procedure.

8.9.2.2 Test procedure

To demonstrate the ability of the access control unit to comply with requirements in Table 8, line 2, perform the following steps:

1) A battery of the maximum capacity recommended by the equipment manufacturer shall be used.
2) Discharge the battery to its final voltage at a discharge current of $I_d = C/20$ A for lead acid type batteries, (or $I_d = C/10$ A for nickel cadmium type batteries), where C is the rated ampere hour capacity of the battery, given by the battery manufacturer.
3) For other battery types, the discharge current shall be that for which the battery manufacturer specifies the rated capacity.
4) Charge the battery for 72 hours with the appropriate charger connected to the nominal mains (V_n) while the power supply output is loaded by I_{max}.
5) Repeat the procedure as in step 2) above and measure the discharge time (T_1) in hours.
6) Charge the battery again for 24 hours at V_n while the access control system outputs are loaded by I_{max}.
7) Discharge the battery again to its final voltage at a discharge current as in step 2) above and measure the discharge time (T_2) in hours.

8.9.2.3 Criteria for compliance

The product of the discharge time T_1 and the discharge current I_d shall be not less than:

a) 100 % of the rated capacity of the battery after charging for 72 hours, and
b) 80 % of the rated capacity of the battery after charging for 24 hours.

8.9.3 Test for low or missing battery condition

8.9.3.1 Object of the test

To demonstrate the means are provided to monitor and signal a low battery condition, as required by Table 8, line 3.

8.9.3.2 Test procedure

The following procedure shall be applied to access control systems incorporating standby batteries:

1) Where appropriate replace the standby batteries with a variable supply power set to the recommended nominal supply voltage (V_{nom}).

   NOTE Some types of battery power source cannot be simulated by the substitution of a variable power supply e.g. lithium batteries. Where necessary, alternative methods to demonstrate compliance are permitted provided the applicant and the test laboratory agree.

2) Confirm correct operation of the access control system by applying the reduced functional test.
3) Slowly lower the level of V_{nom} at a rate of approximately 10 mV/s until a low battery condition is indicated on a local display and/or at the monitoring console.
4) Record the voltage at which the low battery condition indication is given (V_{low}) and apply the reduced functional test.
5) Remove the standby batteries from the access control system entirely and repeat step 4).

8.9.3.3 Criteria for compliance

The access control system shall have signalled a battery trouble indication, alert and logged event in response to a low battery voltage condition before correct operation is prevented. The access control system shall continue to meet the requirements of the reduced functional test whilst the operating voltage is at V_{low}. A battery trouble indication, alert and logged event shall be given upon detection of a missing battery.

8.10 Environmental and EMC (immunity) tests

8.10.1 Test procedure

The applicable EMC and environmental tests specified in Table 9 shall be conducted as follows:

1) The test apparatus and the test procedures shall be as described in IEC 62599-1 and IEC 62599-2. Apply the tests indicated in Table 9.
2) Unless otherwise indicated in the test procedure, the tests shall be carried out at the rated supply voltage for the component.
3) The levels of severity to be applied are defined by four levels from environmental Class I to environmental Class IV:
   a) Class I: indoor but restricted to residential/office environment (e.g. living rooms and offices);
   b) Class II: indoor in general (e.g. sales floors, shops, restaurants, stairways, manufacturing and assembly areas, entrances and storage rooms);
   c) Class III: outdoor but sheltered from direct rain and sunshine or indoor with extreme environmental conditions (e.g. garages, lofts, barns and loading bays);
   d) Class IV: outdoor in general.
4) System interconnections for test purposes (i.e. to inputs and outputs) shall be made with unscreened cables, unless the manufacturer's installation data specifies that only screened cables shall be used.

5) Where the equipment has a number of identical types of inputs or outputs, then the tests shall be applied at least to one input and one output representative of each type.

8.10.2 Initial measurements

In addition to the criteria for compliance specified in IEC 62599-1 and IEC 62599-2, the functional test of 8.2 shall be applied during the initial measurements.

8.10.3 State of the specimen during conditioning

Mount the specimen(s) in accordance with the manufacturer's instructions and connect to suitable power supply equipment as recommended in the documentation supplied with the electronic access control system.

8.10.4 Conditioning

The following measures shall be observed while conducting the tests required in Table 9:

1) The test specimens shall be exposed to the conditioning and tests specified in Table 9 using the methods described in IEC 62599-1 and IEC 62599-2.
2) The impact operational conditioning shall be applied to all components of the access control system. However, impacts shall not be applied directly to displays (e.g. liquid crystal displays) or other types of visible indicators.
3) Electrostatic discharges shall be applied only to parts of the access control equipment likely to be accessible to the end user when installed as a system.
4) Fast transient bursts shall be applied to the a.c. mains lines by the direct injection method and to the other inputs, signal, data and control lines by the capacitive clamp method.

8.10.5 Measurement during conditioning

Monitor the specimen during the conditioning period to detect any access granted, alerts or fault signals.

8.10.6 Final measurements

In addition to the criteria for compliance specified in IEC 62599-1 and IEC 62599-2, the functional test of 8.2 shall be applied during the initial and final measurements.

8.10.7 Criteria for compliance

8.10.7.1 Operational tests

The access control system shall not unintentionally grant access, generate alert, tamper, fault or other signals or messages or change from one mode to another and shall continue to function normally when subjected to the specified range of environmental and EMC conditions.

8.10.7.2 Endurance tests

The access control system shall pass the reduced functional test after being subjected to the specified range of environmental conditions.

8.11 Test report

The test report shall contain as a minimum the following information:

a) identification of the test specimen, build status and firmware/software versions;
b) reference to this part of IEC 60839;
c) the classification of the evaluated component(s) of the access control system;
d) results of the assessment of the requirements of this part of IEC 60839;

e) results of the tests, and any other data, as specified in the individual tests;

f) conditioning period and the conditioning atmosphere;

g) details of the supply and monitoring equipment and the response criteria;

h) details of any deviation from this part of IEC 60839 or from the International Standards to which reference is made, and details of any operations regarded as optional.

9 Documentation and marking

9.1 Documentation

The manufacturer shall prepare installation and user documentation, which shall be provided together with the access control unit. This shall comprise at least the following:

a) general description of the equipment, including a list of the
   - mandatory functions for the grade to which the equipment complies;
   - optional functions of this part of IEC 60839;

b) technical specifications of the inputs and outputs of the access control unit, sufficient to permit an assessment of the mechanical, electrical, and software compatibility with other components of the system, including where relevant:
   - the power requirements for recommended operation;
   - the maximum number of access points, releasing devices;
   - the maximum and minimum electrical ratings for each input and output;
   - information on the communication parameters employed on each transmission path;
   - recommended cable parameters for each transmission path;
   - fuse ratings;

c) installation information, including:
   - operating temperature and humidity range;
   - environmental class;
   - IP/IK rating to which the equipment complies;
   - mounting instructions;
   - instructions for connecting the inputs and outputs;

d) configuring and commissioning instructions;

e) operating instructions;

f) service information.

The manufacturer shall prepare design documentation, which shall be submitted to the testing authority together with the access control equipment. This documentation shall include drawings, parts lists, block diagrams, circuit diagrams and a functional description to such an extent that compliance with this part of IEC 60839 may be checked and that a general assessment of the mechanical and electrical design is made possible.

9.2 Marking

The access control system component shall be marked with the following information:

a) the standard to which the component claims compliance (i.e. IEC 60839-11-1);

b) the component type (e.g. access control unit, card reader, etc.);

c) the name or trademark of the manufacturer or supplier;

d) the grade;

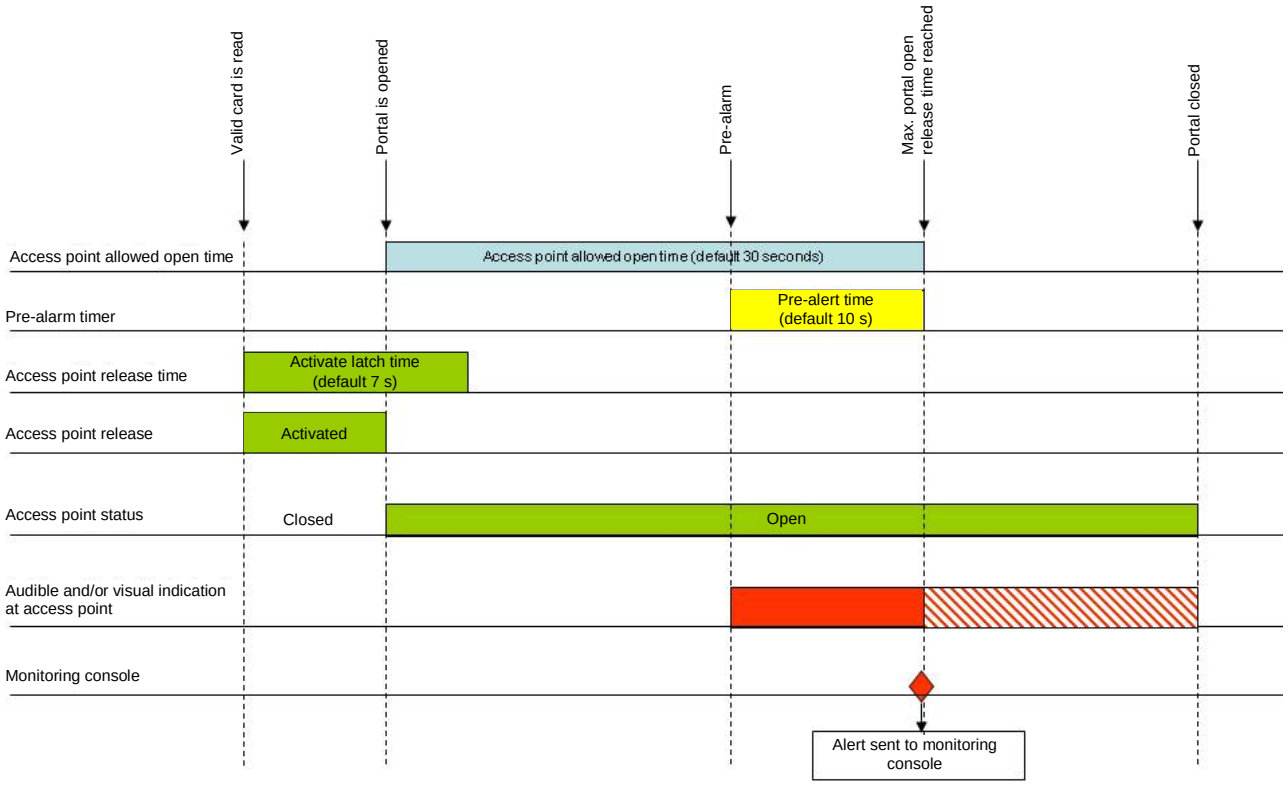
e) the environmental class;

f) the date of manufacture or batch number or serial number.

The marking shall be legible, durable and unambiguous. When space for marking of and access control system component is limited, codes may be used providing these are described in the associated component documentation. When insufficient space is available for codes the component shall include means of identification which allows cross reference to documentation providing the required information.

Annex A
(normative)

Timing diagram



IEC 926/13

NOTE The pre-alert time can be considered as being part or following the portal allowed open time. This can affect the time settings which have to be in accordance with Table 2 requirements.

The local audible and/or visible pre-alert indication can end at the time the alert is sent to the monitoring console or when the portal is closed.

Figure A.1 – Timing diagram

Bibliography

IEC 60839-11-2, *Alarm and electronic security systems – Part 11-2: Electronic access control systems – Application guidelines*

IEC 60950-1, *Information technology equipment – Safety – Part 1: General requirements*

IEC 61000-6-1, *Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity for residential, commercial and light-industrial environments*

IEC 61000-6-3, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La présente Norme internationale CEI 60839-11-1 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme et de sécurité électroniques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/410/FDIS	79/416/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série des CEI 60839, publiées sous le titre général *Systèmes d'alarme et de sécurité électroniques*, est disponible sur le site Internet de la CEI.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente norme fait partie intégrante de la série CEI 60839, qui comprend les parties suivantes:

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

Partie 11-2: Systèmes de contrôle d'accès électronique – Lignes directrices d'application

La présente partie de la CEI 60839 décrit les exigences générales concernant les fonctionnalités des systèmes de contrôle d'accès électronique (EACS) destinés à être utilisés dans les applications de sécurité. La conception, la planification, l'installation, le fonctionnement et la maintenance font partie intégrante des lignes directrices d'application de la CEI 60839-11-2[1]. L'analyse des risques ne fait pas partie intégrante de la présente norme et les niveaux de risque sont donnés à des fins informatives uniquement.

Un système de contrôle d'accès électronique consiste en un ou plusieurs composants qui, lorsqu'ils sont interconnectés, satisfont aux critères de fonctionnalité indiqués dans la présente norme.

La présente norme définit différents niveaux de sécurité, ainsi que les fonctionnalités du système de contrôle d'accès associé à chacun de ces niveaux. Elle inclut également les critères minimum de conformité environnementale et CEM, selon le cas, pour les composants du système de contrôle d'accès électronique dans chaque niveau.

Lorsqu'une partie d'un système de contrôle d'accès électronique (par exemple, interface de points d'accès) fait partie intégrante d'un système d'alarme (anti-intrusion ou hold-up, télévision en circuit fermé, etc.), elle doit également satisfaire aux exigences appropriées des normes CEI applicables. Les fonctions complémentaires aux fonctions obligatoires spécifiées dans la présente norme peuvent être intégrées au système de contrôle d'accès électronique, à condition qu'elles permettent de satisfaire aux exigences de la présente norme

La présente norme internationale s'applique également aux systèmes de contrôle d'accès qui partagent les moyens de reconnaissance, détection, déclenchement, interconnexion, contrôle, communication, signal d'alerte et alimentation avec d'autres applications. Il convient que le fonctionnement d'un système de contrôle d'accès ne soit pas altéré par d'autres applications.

Un système de contrôle d'accès électronique peut comporter un nombre indéfini de points d'accès. La présente norme traite de la classification des classes de sécurité pour chaque point d'accès.

Il est possible d'évaluer la conformité de chaque composant du système de contrôle d'accès électronique par rapport à la présente norme sous réserve de l'application de toutes les exigences pertinentes.

Les exigences spécifiques concernant les actionneurs des points d'accès, tels que les portiers automatiques, dispositifs de verrouillage électroniques, tourniquets et barrières électroniques, sont incluses dans d'autres normes.

---

1 A l'étude.

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

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

1 Domaine d'application

La présente partie de la CEI 60839 spécifie les exigences minimales de fonctionnalités et de performances, ainsi que les méthodes d'essai applicables aux systèmes et composants de contrôle d'accès électronique utilisés pour un accès physique (entrée et sortie) dans et autour des bâtiments et de zones protégées. Elle n'inclut pas les exigences concernant les actionneurs et capteurs de points d'accès.

La présente norme n'est pas destinée à couvrir les exigences concernant la transmission hors lieux associée aux signaux d'alarme anti-intrusion ou anti-hold-up.

La présente norme s'applique aux systèmes et composants de contrôle d'accès électronique destinés à être utilisés dans les applications de sécurité pour l'autorisation d'accès, et inclut les exigences concernant l'enregistrement, l'identification et le contrôle de l'information.

La norme comprend les éléments suivants:

– Un modèle théorique et une architecture système.
– Des critères couvrant:
  - la classification basée sur les fonctionnalités et capacités de performances;
  - les exigences concernant les interfaces de points d'accès;
  - les exigences concernant l'indication et l'annonce (affichage, alerte, enregistrement);
  - le signalement et la neutralisation d'agression;
  - les exigences concernant la reconnaissance;
  - les exigences concernant l'autoprotection des systèmes;
  - la communication entre les composants du système de contrôle d'accès électronique et les autres systèmes.
– Les exigences concernant les conditions d'environnement (utilisation en intérieur/extérieur) et la compatibilité électromagnétique.
– Les méthodes d'essai.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60068-1, *Essais d'environnement – Partie 1: Généralités et guide*

CEI 60529, *Degrés de protection procurés par les enveloppes (Code IP)*

CEI 62262, *Degrés de protection procurés par les enveloppes de matériels électriques contre les impacts mécaniques externes (Code IK)*

CEI 62599-1, *Systèmes d'alarme – Partie 1: Méthodes d'essais d'environnement*

CEI 62599-2, *Systèmes d'alarme – Partie 2: Compatibilité électromagnétique – Exigences relatives à l'immunité des composants de systèmes d'alarme de détection d'incendie et de sécurité*

CEI 62642-1, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 1: Exigences système*

CEI 62642-6, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 6: Alimentation*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions suivants s'appliquent.

3.1
état anormal
écart par rapport au mode de fonctionnement prévu

3.2
accès
accès physique
action d'entrée (ou de sortie) d'une zone de sécurité contrôlée

3.3
unité de contrôle d'accès
contrôleur
partie d'un système de contrôle d'accès en interface avec les lecteurs, dispositifs de verrouillage et capteurs, qui émet une décision d'autorisation ou de refus d'accès par le biais d'un accès contrôlé

3.4
décision d'accès
action consistant à comparer l'information avec les règles préétablies afin de déterminer l'autorisation ou le refus d'accès

3.5
niveau d'accès
ensemble de règles permettant de déterminer les conditions dans lesquelles un identifiant a autorisé l'accès à un ou plusieurs accès contrôlés, et qui peuvent comporter des conditions de passage particulières telles que les périodes spécifiques d'ouverture autorisée du ou des accès contrôlés

3.6
point d'accès
accès contrôlé
entrée/sortie physique à laquelle l'accès peut être contrôlé par une porte, un tourniquet ou toute autre barrière de sécurité

3.7
dispositif d'activation d'un point d'accès
activation d'un accès contrôlé
fonction d'un système de contrôle d'accès électronique associée à la libération ou à la protection d'un accès contrôlé selon les règles préétablies, et subordonnée aux droits d'accès des utilisateurs

3.8
neutralisation d'un point d'accès
neutralisation de l'activation d'un accès contrôlé
émission effective d'une commande manuelle de contournement du mode de fonctionnement pré-configuré (c'est-à-dire libération/protection/blocage) d'un point d'accès

3.9
dispositif d'activation d'un point d'accès
dispositif d'activation d'un accès contrôlé
partie d'un système de contrôle d'accès en interface avec une unité de contrôle d'accès qui libère et protège un accès contrôlé selon les règles préétablies

3.10
ouverture forcée d'un point d'accès
ouverture forcée d'un accès contrôlé
signal d'alerte généré en cas d'ouverture d'un point d'accès sans autorisation dudit accès

3.11
interface des points d'accès
interface d'un accès contrôlé
dispositifs ou circuits contrôlant la libération et la protection d'un point d'accès

3.12
changement d'état d'un point d'accès
changement d'état d'un accès contrôlé
événement déclenché par le changement d'un point d'accès de l'état verrouillé à l'état déverrouillé ou de l'état déverrouillé à l'état verrouillé

3.13
dispositif de verrouillage d'un point d'accès
dispositif de verrouillage d'un accès contrôlé
ensemble associé au point d'accès, qui assume la fonction de maintien en position fermée d'un point d'accès et qui est en mesure de libérer le point d'accès conformément aux règles préétablies

3.14
temps d'ouverture d'un point d'accès
temps d'ouverture d'un accès contrôlé
temps maximal d'ouverture d'un point d'accès après autorisation de l'accès et avant le déclenchement d'une alerte pour cause de temps d'ouverture trop long d'un point d'accès

3.15
alerte pour cause de temps d'ouverture trop long d'un point d'accès
alerte pour cause de temps d'ouverture trop long d'un accès contrôlé
signal généré en cas de dépassement du temps d'ouverture d'un point d'accès après autorisation de l'accès

3.16
libération d'un point d'accès
libération d'un accès contrôlé
signal indiquant l'autorisation de l'accès au dispositif de verrouillage d'un point d'accès

3.17
capteur d'un point d'accès
capteur d'un accès contrôlé
composant électronique utilisé pour contrôler l'état d'ouverture ou fermeture d'un point d'accès, ou l'état verrouillé/déverrouillé d'un dispositif de verrouillage, voire l'état de protection/absence de protection d'une serrure électromagnétique ou d'une plaque d'armature

3.18
demande d'accès
lecture d'un identifiant au niveau de l'accès contrôlé, qui lance le processus de décision en vue de l'autorisation d'entrée ou de sortie de la zone contrôlée par l'accès contrôlé

Note 1 à l'article: Voir dispositif de demande de sortie.

3.19
temps de réponse à une demande d'accès
temps nécessaire au système pour répondre à une demande d'accès, de la présentation correcte de l'identifiant à l'activation du dispositif répondant

Note 1 à l'article: Le temps de réponse à une demande d'accès remplace le terme temps d'authentification.

3.20
équipement annexe
tout composant d'un système de contrôle d'accès électronique autre que l'unité de contrôle d'accès

3.21
alarme
<système de contrôle d'accès> condition requérant l'évaluation ou l'intervention d'un individu

Note 1 à l'article: Utilisée souvent dans un système de contrôle d'accès électronique au sens d'une alerte.

3.22
alerte
fonctionnalité d'un système de contrôle d'accès électronique associée à l'activation d'un indicateur destiné à guider l'évaluation par un individu

3.23
alerte accès contrôlé
signal visuel et/ou sonore qui accompagne l'action de guidage de l'accès contrôlé visant à fermer le point d'accès/accès contrôlé ouvert et à mettre un terme à la condition d'alerte

3.24
inhibition d'alerte
contournement
fonction système empêchant un évènement de générer une alerte

Note 1 à l'article: L'évènement inhibition d'alerte peut être enregistré ou non.

Note 2 à l'article: L'activation/la désactivation de l'inhibition d'alerte s'effectue manuellement par l'opérateur système, accès contrôlé par accès contrôlé.

3.25
équipement auxiliaire
équipement individuel à des fins de contrôle supplémentaire, conçu pour être intégré ou ajouté à un système de contrôle d'accès électronique par le personnel d'entretien qualifié et qui ne doit pas empêcher les exigences de base du système de contrôle d'accès d'être atteintes

3.26
annonce
présentation des informations aux utilisateurs, aux responsables ou à d'autres systèmes réalisée par les fonctionnalités AFFICHAGE, ALERTE et ENREGISTREMENT d'un système de contrôle d'accès électronique

3.27
anti retour
mode de fonctionnement requérant la validation de l'utilisateur lorsqu'il quitte une zone de sécurité contrôlée, afin de pouvoir y pénétrer une autre fois et inversement

Note 1 à l'article: Se reporter également à anti retour rigide, anti retour souple, anti retour général et anti retour temporisé.

3.28
anti retour de zone contrôlée
mode de fonctionnement requérant la présence de l'utilisateur dans une zone de sécurité contrôlée désignée, afin de pouvoir pénétrer dans une autre zone de sécurité contrôlée

3.29
neutralisation du dispositif anti retour
désactivation du dispositif anti retour
fonction système de désactivation du dispositif anti retour

3.30
anti-passage en double
fonction qui empêche ou détecte la tentative d'accès de deux personnes ou entités ou plus, en utilisant uniquement un seul ensemble d'identifiants

3.31
plaque d'armature
plaque métallique conçue pour être utilisée avec une serrure électromagnétique

3.32
authentification
processus utilisé pour vérifier l'intégrité de la reconnaissance des identifiants

3.33
biométrie
biométrique, adj
toute caractéristique physiologique ou personnelle mesurable unique utilisée comme identifiant permettant de reconnaître et de vérifier l'identité de la dynamique d'un individu

EXEMPLE: La biométrie inclut mais sans s'y limiter l'empreinte digitale, la géométrie de la main ou du visage, la reconnaissance rétinienne/oculaire, la reconnaissance faciale, vocale, la dynamique de la signature ou de la saisie au clavier.

3.34
accès bloqué
blocage du passage par un point d'accès même en cas de présentation d'identifiants valides

3.35
événements tamponnés
événements à archivage provisoire en attente de transmission pour un traitement ultérieur

3.36
carte
type de jeton

3.37
cause de refus
justification d'un refus d'accès

EXEMPLE: Les causes de refus d'accès incluent: le privilège d'accès ne comprenant pas l'accès contrôlé, la période, le jour, les congés/jours fériés et le code d'installation particuliers; l'information mémorisée incorrecte ou

non fournie dans les délais; la violation du dispositif anti retour, la fin de validité de l'identifiant ou identifiant non effectif ou non programmé dans le système.

3.38
composant
toute partie d'un système de contrôle d'accès électronique

EXEMPLE: Inclut les unités de contrôle d'accès, lecteurs, actionneurs et capteurs de points d'accès, claviers numériques, dispositifs de demande de sortie, et tout sous-ensemble y afférent.

3.39
configurable
caractéristique d'activation et de désactivation d'une fonction d'un système de contrôle d'accès électronique ou valeurs de paramètres système à modifier selon ce que les règles préétablies permettent

3.40
configuration
processus ou résultat de l'activation/désactivation des fonctions système et/ou du changement des valeurs de paramètres selon ce que les règles préétablies permettent

3.41
mode de configuration
état de l'unité de contrôle d'accès pendant lequel les fonctions supportées par le système peuvent être activées/désactivées ou pendant lequel les valeurs des paramètres peuvent être réglées ou modifiées comme nécessaire

3.42
identifiant
information mémorisée ou contenue dans un jeton

EXEMPLE: L'information inclut une image biométrique utilisée pour identifier un individu souhaitant utiliser un système de contrôle d'accès afin d'authentifier un utilisateur.

3.43
réintégration d'identifiant
commande de réactivation d'un identifiant ayant enfreint les règles anti retour

Note 1 à l'article: Voir réintégration et réintégration générale.

3.44
suspension de l'identifiant
fonction d'un système de contrôle d'accès électronique autorisant l'invalidation provisoire d'un identifiant

Note 1 à l'article: La suspension est appliquée au cas par cas, habituellement dans des situations de perte des identifiants.

3.45
suivi d'identifiant
fonction qui suit les mouvements, en temps réel, d'identifiants particuliers (numéros d'identification personnelle, jetons ou biométrie) à l'intérieur et à l'extérieur des accès contrôlés

Note 1 à l'article: Programmée par l'administrateur système, cette fonction déclenchera une alerte, un enregistrement ou un affichage à l'occasion de chaque utilisation d'un identifiant particulier (numéro d'identification personnelle, jeton ou biométrie) au niveau de tout accès contrôlé comme défini par l'administrateur système.

3.46
compteur d'utilisation d'identifiant
fonction utilisée pour les parcs de stationnement et pour d'autres applications particulières, qui comptabilise le nombre d'utilisations et détermine la fin de validité de l'identifiant

3.47
authentification des données
processus utilisé pour vérifier l'intégrité des données transmises

Note 1 à l'article: L'intégrité des données est assurée tant qu'il ne se produit ni destruction accidentelle ou malveillante, ni modification ni suppression.

3.48
validation du système d'entrée de données
notification de l'administrateur système de l'acceptation/du rejet du système des données individuelles entrées en mode programmation

3.49
pêne dormant
dispositif de verrouillage qui engage et dégage un pêne par l'application d'une force électrique, hydraulique ou pneumatique

3.50
défaut
paramétrages dans le système de contrôle d'accès électronique fournis par le fabricant qui peuvent être changés ultérieurement

3.51
mode de fonctionnement dégradé
mode de fonctionnement limité des composants de contrôle d'accès lors d'une défaillance de communication

3.52
temps d'alerte
temps qui s'écoule entre le moment où le système de contrôle d'accès électronique reconnaît un changement effectif et le moment où l'alerte qui y est associée est indiquée à la console de commande

3.53
entrées numériques
ensemble des entrées du système de contrôle d'accès électronique, à l'exception des signaux de communication

EXEMPLE: Entrées relatives au contrôle des portes, entrées relatives au capteur, entrées d'autres systèmes indiquant leur état, etc.

3.54
affichage
fonctionnalité d'un système de contrôle d'accès électronique associée à la présentation visuelle de l'information dans le système

3.55
identifiant double
identifiant multiple
fonction des systèmes de contrôle d'accès électronique, qui exige deux demandes d'accès autorisées séquentielles ou plus dans une période configurable en vue de l'autorisation d'accès

3.56
occupation double
occupation multiple
fonction des systèmes de contrôle d'accès électronique, qui compte le nombre d'utilisateurs entrant et quittant une zone de sécurité contrôlée et qui autorise l'entrée/sortie uniquement lorsque au moins deux utilisateurs autorisés pénètrent/demeurent dans la zone de façon permanente

3.57
alerte d'agression
fonction d'un système de contrôle d'accès électronique associée à l'avertissement silencieux déclenché par les utilisateurs du système qui saisissent un code d'agression lorsqu'ils sont soumis à une activité coercitive, destinée à autoriser l'accès aux personnes non autorisées

3.58
signalement d'agression
fonction consistant à générer une alerte d'agression au niveau de la console de commande

3.59
serrure complète électrique
serrure mécanique conçue pour être libérée également de manière électrique

Note 1 à l'article: Elle peut également comporter un dispositif de libération mécanique, une unité de contrôle d'accès intégrée et/ou un lecteur ou clavier numérique.

3.60
gâche électrique
dispositif commandé à distance qui libère la languette de la gâche permettant ainsi l'ouverture de l'accès contrôlé sans déverrouiller la serrure

3.61
barre anti-panique électrique
barre anti-panique mécanique conçue pour être libérée également de manière électrique

3.62
serrure électromagnétique
serrure électrique, qui se verrouille ou se déverrouille par l'activation ou la désactivation d'un électroaimant, couplé magnétiquement à une plaque d'armature

3.63
système de contrôle d'accès électronique
système de contrôle d'accès
système conçu pour accorder aux personnes ou aux entités autorisées, le droit d'entrée et/ou sortie d'une zone de sécurité contrôlée et refuser ce droit d'entrée et/ou sortie aux individus ou entités non autorisés

Note 1 à l'article: L'étendue du contrôle d'entrée/sortie peut inclure le compte-rendu et l'enregistrement de l'activité associée.

3.64
commande de manœuvre
fonction des systèmes de contrôle d'accès électronique qui limite l'utilisation des ascenseurs ou des cabines de monte-charge

3.65
entité
tout objet mobile auquel des droits d'accès ont été octroyés

EXEMPLE: Véhicule, etc.

3.66
événement
changement intervenant au sein d'un système de contrôle d'accès électronique

3.67
taux supportable d'erreurs
pourcentage de reconnaissance erronée des utilisateurs dont l'accès a été autorisé

3.68
panne
condition de fonctionnement non conforme d'un composant système selon la conception

3.69
code d'installation
numéro intégré au jeton en cours de fabrication ou de codage, destiné à identifier le système pour lequel le jeton est valable (par exemple, code système, site ou client)

EXEMPLE: Code système, site ou client.

3.70
réintégration
commande appliquée en cas d'utilisation du dispositif anti retour pour la réinitialisation des identifiants à l'état "emplacement inconnu" après une violation anti retour rigide

Note 1 à l'article: Lors de l'utilisation suivante des identifiants, leur état est corrigé automatiquement indépendamment du fait qu'ils soient utilisés pour une entrée ou une sortie. La commande peut se rapporter à un seul identifiant (voir réintégration de carte) ou à tous les identifiants à la fois (voir réintégration générale), comme suite à une évacuation d'urgence de l'installation.

3.71
actionneur sur châssis
mécanisme sur châssis, qui manipule un composant d'un mécanisme de verrouillage coopérant d'une porte (manœuvre telle que le désengagement du verrou hors de la gâche) en réponse aux signaux émis par un organe d'entrée ou un dispositif de commande, permettant l'ouverture de l'accès contrôlé sans déverrouillage de la serrure

3.72
autorisation de libre accès
condition de libération d'un accès contrôlé sans aucune décision conformément aux règles préétablies

Note 1 à l'article: Voir également autorisation de libre accès temporisé, autorisation de libre accès jusqu'à une commande ultérieure du système, et autorisation unique de libre accès.

3.73
autorisation de libre accès jusqu'à une commande ultérieure du système
fonction système autorisant l'opérateur système à libérer et à protéger à nouveau un accès contrôlé sans aucune reconnaissance conformément aux règles préétablies

3.74
anti retour général
caractéristique système qui applique les règles anti retour à tout point d'accès autorisé d'une zone contrôlée même lorsque le lecteur est connecté à une unité de contrôle d'accès différente

3.75
réactivation d'identifiant du dispositif anti retour général
commande appliquée en cas d'utilisation du dispositif anti retour pour la réinitialisation de tous les identifiants à l'état "emplacement inconnu" après une défaillance du système

Note 1 à l'article: Lors de l'utilisation suivante d'un identifiant, son état est corrigé automatiquement indépendamment du fait qu'il soit utilisé pour une entrée ou une sortie.

3.76
documents graphiques
dessins, cartes ou images fournissant des aides visibles destinées à venir à l'appui de l'évaluation des conditions

3.77
anti retour rigide
caractéristique système qui génère une alerte et refuse tout autre accès à un identifiant particulier suite à la violation des règles anti retour

3.78
heure locale
heure du pays dans lequel se situe chaque unité de contrôle d'accès

3.79
enregistrement
fonction d'un système de contrôle d'accès électronique associée à l'enregistrement et à la récupération des changements (événements) intervenant dans le système

3.80
niveaux d'accès logiques, pl
droits d'accès, pl
capacité des opérateurs à exécuter des fonctions au sein du système de contrôle d'accès électronique telles que la configuration ou l'administration, les termes classés d'autorisation/responsabilités de l'opérateur

3.81
sas de sécurité
combinaison de deux accès contrôlés ou plus devant être utilisés de manière séquentielle afin de pouvoir accéder à une zone de sécurité contrôlée

Note 1 à l'article: La libération d'un accès contrôlé supplémentaire dépend de la fermeture de l'accès contrôlé précédent utilisé, ainsi que de la reconnaissance des identifiants valides.

3.82
horloge maîtresse
dispositif général de synchronisation horaire (horloge) d'un système de contrôle d'accès électronique en présence de deux unités de contrôle d'accès ou plus

3.83
information mémorisée
information connue de l'utilisateur

EXEMPLE: Code PIN.

3.84
console de commande
composant fonctionnel constitué de dispositifs utilisés comme interface de contrôle, d'enregistrement et de signalisation pour l'opérateur d'un système de contrôle d'accès électronique

3.85
accès multiple
double accès
fonction des systèmes de contrôle d'accès électronique, qui exige deux demandes d'accès autorisées séquentielles ou plus dans une période configurable en vue de l'autorisation d'accès

3.86
condition normale
système de contrôle d'accès entièrement fonctionnel et en mesure de traiter tous les événements dans le respect des règles préétablies

3.87
neutraliser, v
contournement d'une fonction, généralement de manière provisoire

EXEMPLE: Pour désactiver provisoirement la fonction anti retour.

3.88
contrôle de présence
confirmation du nombre (max., min.) de personnes présentes dans une zone de sécurité contrôlée

3.89
règles préétablies
ensemble de principes de fonctionnement prédéfinis grâce auxquels le système de contrôle d'accès électronique fonctionne

3.90
zone protégée
zone contrôlée
zone définie par une limite physique, par laquelle le passage est contrôlé au moyen d'un ou de plusieurs points d'accès

3.91
lecteur
dispositif d'entrée des identifiants

EXEMPLE: Lecteur de jetons ou de cartes, lecteur biométrique, etc.

3.92
suivi de lecteur
fonction des systèmes de contrôle d'accès électronique autorisant le suivi des activités de tous les identifiants au niveau d'un lecteur spécifique

3.93
reconnaissance
action d'identification des utilisateurs autorisés qui demandent un accès par la comparaison des données d'identifiant présentées avec les données d'identifiant enregistrées

3.94
synchronisation de libération
période de déverrouillage des points d'accès par le système selon les règles préétablies

3.95
dispositif de demande de sortie
dispositif associé à un point d'accès permettant une sortie libre

3.96
RFID
dispositif sans contact émettant et/ou recevant des informations d'identifiant par ondes radio

3.97
appel nominal
fonction d'énumération des utilisateurs ou des identifiants enregistrés comme étant situés "DANS" la ou les zones contrôlées par le système de contrôle d'accès électronique

3.98
accès programmé
libre accès temporisé
période au cours de laquelle un système de contrôle d'accès électronique ne contrôle ni l'accès ni la sortie, comme déterminé par les règles préétablies

3.99
autorisation unique de libre accès
fonction système autorisant l'opérateur système à libérer un accès contrôlé sans aucune reconnaissance des identifiants

Note 1 à l'article: Lors de sa fermeture, l'accès contrôlé est automatiquement protégé par le système conformément aux règles préétablies.

3.100
séparation
limitation du franchissement simultané du point d'accès par un seul utilisateur

3.101
anti retour souple
caractéristique système qui, lors de l'autorisation d'accès, génère une alerte suite à la violation des règles anti retour

3.102
mode autonome
mode de fonctionnement du système de contrôle d'accès en l'absence de communication entre l'unité de contrôle d'accès et la console de commande

3.103
mode de surveillance
fonction des systèmes de contrôle d'accès électronique, qui exige qu'une demande d'accès autorisée en mode surveillance soit utilisée avec un autre identifiant pour l'autorisation d'accès

3.104
administrateur système
personne responsable de la détermination et/ou mise en œuvre des règles de traitement du système de contrôle d'accès électronique

3.105
défini par le système
options du système de contrôle d'accès électronique définies selon une valeur fixe (c'est-à-dire programmées en usine) et qui ne peuvent être modifiées dans la pratique par une action de reprogrammation

3.106
opérateur système
personne chargée du fonctionnement de la console de commande du système de contrôle d'accès électronique, ainsi que des tâches de contrôle, et qui peut ou non entrer/éditer des données système

3.107
autoprotection d'un système
fonctionnalité d'un système de contrôle d'accès électronique associée à la prévention, la détection et/ou le signalement d'une altération délibérée et fortuite, et/ou l'ingérence avec le fonctionnement du système

3.108
passage en double
personne ou entité, qui passe un point d'accès sans utiliser d'identifiants, mais par le seul fait de suivre une personne ou une entité dont l'accès a été autorisé

3.109
protection contre la fraude
méthode utilisée pour protéger un système de contrôle d'accès ou une partie de ce dernier contre toute ingérence délibérée

3.110
anti retour temporisé
caractéristique d'un système assurant le suivi d'une demande d'accès par identifiant individuelle à une zone donnée pour laquelle un accès autorisé n'a pas été suivi par une sortie autorisée, ou une sortie autorisée n'a pas été suivie par un accès autorisé dans une période prédéterminée

Note 1 à l'article: Cette caractéristique évite l'autorisation d'une seconde demande d'accès ultérieure délivrée à la même carte dans la même zone, préalablement à l'expiration d'une période anti retour configurable par l'utilisateur.

3.111
autorisation temporisée de libre accès
zone de temps réglable lorsque la condition de libération de l'accès contrôlé sans aucune reconnaissance des identifiants est admise

3.112
plage horaire
intervalle de temps entre deux moments donnés indiquant le commencement et la fin d'une période valide dans une zone de temps

3.113
zone de temps
une ou plusieurs plages horaires combinées avec des informations calendaires

3.114
jeton
dispositif portable contenant un identifiant unique lisible pouvant être associé aux données et droits d'accès d'un utilisateur mémorisés dans le système de contrôle d'accès électronique

3.115
transaction
événement qui correspond à la libération d'un point d'accès suite à la reconnaissance de l'identité de l'utilisateur

3.116
tourniquet
accès contrôlé conçu pour limiter physiquement le passage à une seule personne à la fois

3.117
utilisateur
personne qui demande à passer un point d'accès

3.118
information d'identification
identité de l'utilisateur
information qui est transférée directement ou via un jeton, par l'utilisateur, à l'équipement de reconnaissance

3.119
accès avec escorte des visiteurs
fonction de systèmes de contrôle d'accès électronique qui autorise l'accès à une zone, selon un niveau d'accès donné, selon l'utilisation séquentielle des identifiants d'un niveau d'accès spécifique différent

4 Abréviations

Pour les besoins du présent document, les abréviations données dans la CEI 62642-1, ainsi que les abréviations suivantes, s'appliquent.

Abréviations	Français	Anglais
ACS	Système de contrôle d'accès	Access control system
ACU	Unité de contrôle d'accès	Access control unit
APS	Capteur d'un point d'accès	Access point sensor
EACS	Système de contrôle d'accès électronique	Electronic access control system
EEPROM	Mémoire morte programmable effaçable électriquement	Electrically-erasable programmable read-only memory
FAR	Taux supportable d'erreurs	False acceptance rate
ID	Information d'identification	Identification information
RAM	Mémoire vive	Random access memory
REX	Dispositif de demande de sortie	Request-to-exit device
RFID	Identification par radiofréquences ou dispositif d'identification par radiofréquences	Radio frequency identification or radio frequency identification device

5 Modèles théoriques et architecture système

Le système de contrôle d'accès électronique doit inclure, comme approprié à sa configuration spécifique, les fonctions de base suivantes: traitement (A), communication (B), configuration (programmation) (C), interface des points d'accès (D), reconnaissance (E), annonce (F), signalement d'agression (G), interface avec d'autres systèmes (H), autoprotection (I), alimentation (J), interface utilisateur (K):

A Traitement: comparaison des changements survenant dans le système avec les règles préétablies afin de produire des actions prédéfinies.

B Communication: transmission de signaux entre les composants du système de contrôle d'accès afin d'assurer l'application des règles préétablies.

C Configuration (programmation): définition des règles de traitement.

D Interface des points d'accès:

- activation d'un point d'accès: libération et protection d'un accès contrôlé selon les règles préétablies;

- contrôle d'un point d'accès: compte-rendu continu de l'état ouvert/fermé d'un accès contrôlé, et/ou de l'état de libération/protection des dispositifs de protection de l'accès contrôlé;
- neutralisation de l'activation d'un point d'accès: libération/protection d'un accès contrôlé selon les règles préétablies sans aucune reconnaissance.

E Reconnaissance: reconnaissance des utilisateurs autorisés sollicitant un accès.

F Annonce: fonctionnalités d'alerte, d'affichage et/ou d'enregistrement:

- alerte: sous-fonctionnalité d'annonce associée à l'activation d'un indicateur destiné à guider l'évaluation par un individu;
- affichage: sous-fonctionnalité d'annonce associée à la présentation visuelle et/ou sonore des changements se produisant dans le système;
- enregistrement: sous-fonctionnalité d'annonce associée à l'enregistrement et à la récupération des changements se produisant dans le système.

G Signalement d'agression: avertissement silencieux, par les utilisateurs système, des conditions de demande d'accès coercitives permanentes.

H Interface avec d'autres systèmes: partage des fonctionnalités et/ou changements se produisant dans les systèmes.

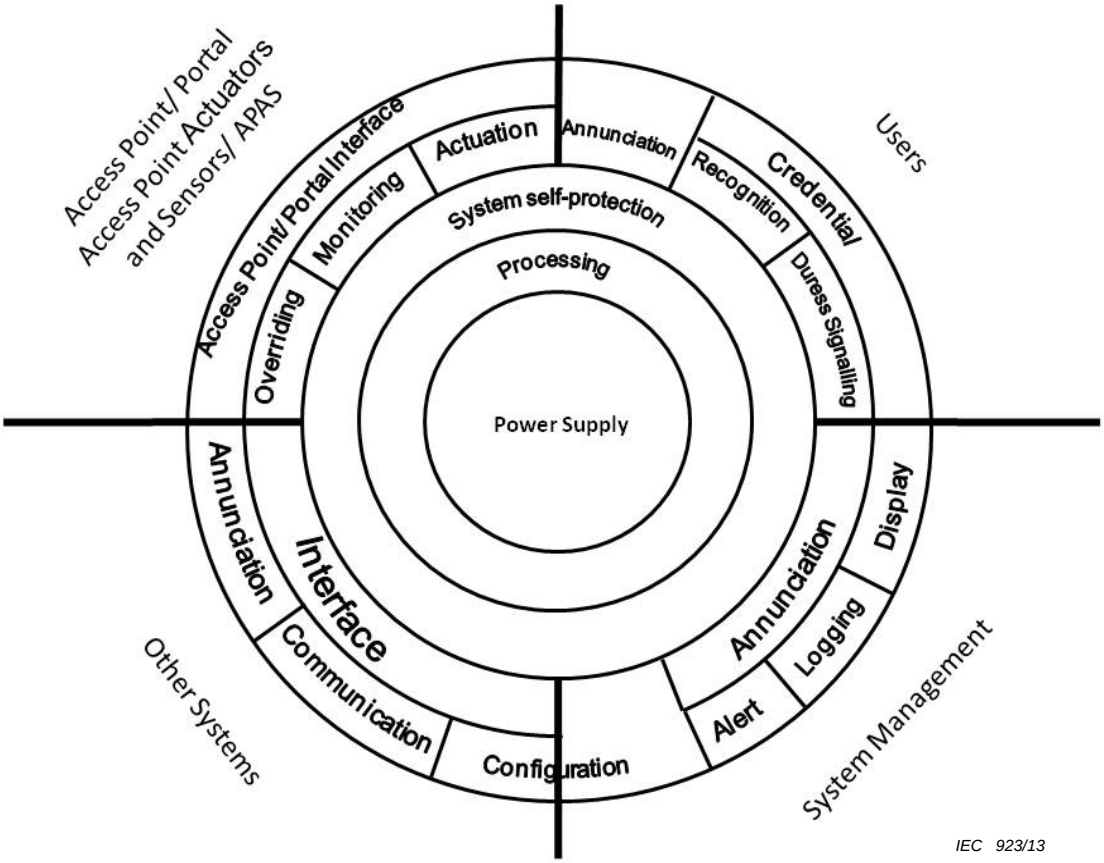
I Autoprotection: prévention, détection et/ou signalement d'une altération délibérée et fortuite, et/ou ingérence avec le fonctionnement du système.

J Alimentation: module de fourniture d'énergie au système de contrôle d'accès. Les exigences d'alimentation définies dans la présente norme ne couvrent pas les besoins en énergie des actionneurs de points d'accès. Lorsqu'une partie d'un système de contrôle d'accès électronique (par exemple, interface des points d'accès) fait également partie intégrante d'un système d'alarme d'intrusion, l'alimentation de cette partie doit satisfaire aux exigences appropriées de la norme CEI 62642-6.

K Interface utilisateur: moyen par lequel l'utilisateur sollicite un accès (par exemple, clavier numérique ou lecteur de jetons) et est informé de l'état d'accès.

Les fonctions complémentaires aux fonctions obligatoires spécifiées dans la présente norme peuvent être intégrées au système de contrôle d'accès électronique, à condition qu'elles n'influent pas sur le fonctionnement correct des fonctions obligatoires.

Le modèle théorique des systèmes de contrôle d'accès électronique et l'architecture système sont illustrés par la Figure 1 et la Figure 2.

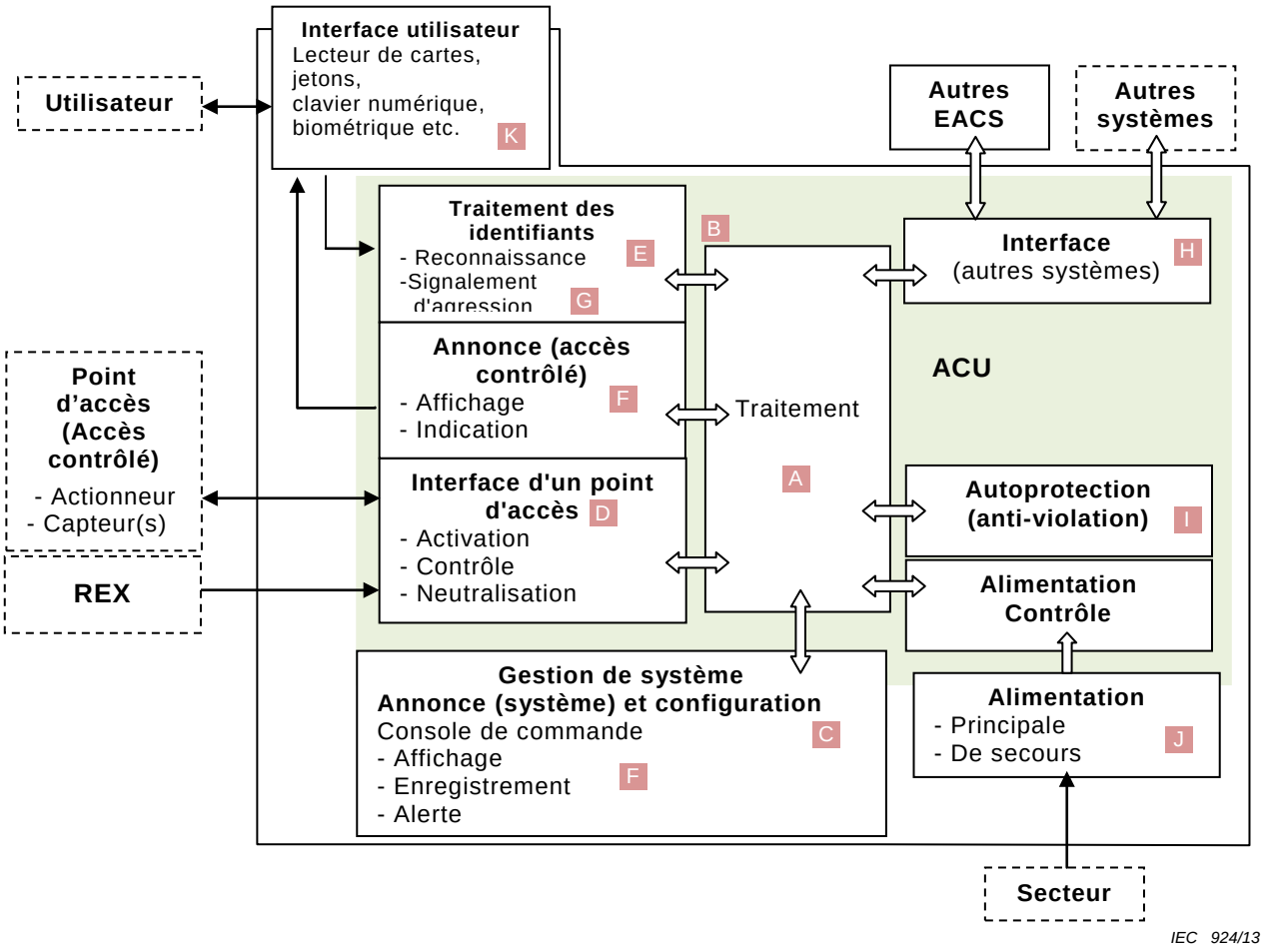


Légende

Anglais	Français
Access point/ portal interface	Point d'accès / interface d'accès contrôlé
Access point / portal	Point d'accès / accès contrôlé
Access point actuators and sensors /APAS	Capteurs et activateurs de point d'accès contrôlé / APAS
Portal	Accès contrôlé
Overriding	Neutralisation
Monitoring	Contrôle
Actuation	Activation
Users	Utilisateurs
Credential	Identifiant
Recognition	Reconnaissance
Annunciation	Annonce
Communication	Communication
Interface	Interface
Duress signalling	Signalement d'agression
Other systems	Autres systèmes
System management	Gestion de système
Configuration	Configuration
Alert	Alerte
Logging	Enregistrement

Anglais	Français
Display	Affichage
System self-protection	Autoprotection du système
Processing	Traitement
Power supply	Alimentation

Figure 1 – Modèle théorique



Les composants entourés de pointillés ne relèvent pas du domaine d'application de la présente norme.

Les fonctions peuvent être réparties dans deux enceintes ou plus ou intégrées dans une seule armoire.

L'annonce et la configuration de la gestion de système peuvent être effectuées par des applications logicielles uniquement. Les exigences minimales concernant la plate-forme matérielle doivent être spécifiées.

Figure 2 – Architecture typique d'un système de contrôle d'accès électronique

6 Exigences concernant les fonctionnalités de performance des systèmes

6.1 Méthodologie et fonctionnalités de classification – Détermination des niveaux de protection

Les exigences concernant les performances des équipements doivent être structurées selon des classes correspondant aux niveaux de protection. Cette structuration s'effectue par classement des fonctionnalités relatives à la sécurité (reconnaissance, activation et contrôle d'un point d'accès, signalement d'agression et autoprotection d'un système) par rapport aux niveaux de risque.

La classification du système de contrôle d'accès doit correspondre à l'une des quatre classes existantes, la classe 1 étant la plus faible et la classe 4 la plus élevée. La classification de sécurité doit être définie pour chaque point d'accès, et ce, pour l'entrée et la sortie à un niveau individuel (voir le Tableau1).

Différentes classes pour les interfaces de points d'accès peuvent être utilisées dans la même installation tant que les fonctions fournies par le système de contrôle d'accès et les identifiants utilisés satisfont au moins aux exigences de la classification de sécurité la plus élevée du ou des points d'accès contrôlés par ce système.

Lorsqu'une fonction est incluse, et par ailleurs facultative dans la norme, pour la classe pour laquelle le composant revendique la conformité, il convient que la documentation indique clairement et de manière explicite la ou les classes supérieures, lorsqu'elles existent, auxquelles ces fonctions sont conformes. Lorsque ces fonctions ne sont pas conformes aux exigences d'une classe supérieure, cette information doit alors être clairement et explicitement indiquée dans la documentation.

Les niveaux de risque sont définis en termes de la valeur des biens nécessitant une protection et de la détermination (connaissance/compétences) ainsi que des méthodes d'agression des personnes qui envisagent de contourner le système (adversaires).

– Classe 1: risque faible. L'adversaire est supposé mal connaître le système de contrôle d'accès et être limité à une gamme restreinte d'outils facilement disponibles. La sécurité physique a pour objectif de décourager et de retarder les adversaires. Les biens ont une valeur limitée et les adversaires en présence abandonneront vraisemblablement toute idée d'agression lorsqu'ils seront confrontés à une résistance minimale.
– Classe 2: risque faible à moyen. L'adversaire est supposé avoir une connaissance limitée du système de contrôle d'accès, ainsi que de l'utilisation d'une gamme générale d'outils et d'instruments portatifs. La sécurité physique a pour objectif de décourager, retarder et détecter les adversaires. Les biens ont une plus grande valeur et les adversaires en présence abandonneront vraisemblablement toute idée de réussite lorsqu'ils s'apercevront qu'ils peuvent être détectés.
– Classe 3: risque moyen à élevé. L'adversaire est supposé bien connaître le système de contrôle d'accès et disposer d'une gamme complète d'outils et d'équipements électroniques portatifs. La sécurité physique a pour objectif de décourager, retarder, détecter et faciliter l'identification des adversaires. Les biens ont une grande valeur et les adversaires en présence peuvent abandonner toute idée de réussite lorsqu'ils s'aperçoivent qu'ils peuvent être identifiés et pris en flagrant délit.
– Classe 4: risque élevé. L'adversaire est supposé avoir la capacité ou disposer des ressources nécessaires à la planification détaillée de l'agression et disposer également d'une gamme complète d'équipements, y compris les moyens de remplacement des composants dans les systèmes de contrôle d'accès. La sécurité physique a pour objectif de décourager, retarder, détecter et faciliter l'identification des adversaires. Les biens ont une très grande valeur et les adversaires en présence peuvent abandonner toute idée de réussite lorsqu'ils s'aperçoivent qu'ils seront identifiés et pris en flagrant délit.

Tableau 1 – Catégorisation des classes

Classe	1	2	3	4
Niveau de risque	Faible	Faible à moyen	Moyen à élevé	Elevé
Application	aspects organisationnels, protection des biens de faible valeur	aspects organisationnels, protection des biens de valeur faible à moyenne	moins d'aspects organisationnels, protection des biens commerciaux de valeur moyenne à élevée	protection principalement des biens commerciaux de très grande valeur ou infrastructure critique
Compétence/connaissances des adversaires/agresseurs	faible compétence, faible connaissance des ACS, aucune connaissance des technologies des jetons et des technologies IT ressources financières faibles pour les agressions	compétence et connaissance moyennes des ACS, faible connaissance des technologies des jetons et des technologies IT ressources financières faibles à moyennes pour les agressions	compétence et connaissance élevées des ACS, connaissance moyenne des technologies des jetons et des technologies IT ressources financières moyennes pour les agressions	compétence et connaissance très élevées des ACS, connaissance élevée des technologies des jetons et des technologies IT ressources financières élevées pour les agressions
Exemples typiques	hôtel	bureaux, petites et moyennes entreprises	secteurs industriel, administratif et financier	secteurs très sensibles (installations militaires, structures gouvernementales, R&D, zones de production critique)

6.2 Exigences concernant les interfaces de points d'accès

6.2.1 Synchronisation de libération de l'accès contrôlé

L'unité de contrôle d'accès doit être capable de déverrouiller les accès contrôlés conformément aux règles préétablies pendant une période définie ou programmable par le système, conformément au Tableau 2. En cas de contrôle de l'état d'un point d'accès, la libération de l'actionneur du point d'accès doit alors s'interrompre en cas d'ouverture de ce même point.

6.2.2 Contrôle d'accès

Un système de contrôle d'accès électronique doit être capable de contrôler l'accès conformément au Tableau 2 et au chronogramme présenté à l'Annexe A. Les exigences du Tableau 2 doivent s'appliquer aux points d'accès individuels conformément à leur catégorie. Les caractéristiques «globales» doivent s'appliquer à tous les points d'accès d'une même catégorie.

Il convient que les systèmes de contrôle d'accès électronique comportent des sorties capables de manœuvrer les serrures électromagnétiques, des gâches électriques, actionneurs sur châssis, pênes dormants électriques, hydrauliques ou pneumatiques et/ou d'autres types d'ensembles de serrures électriques et de barres anti-panique électriques.

6.2.3 Etat des accès contrôlés

6.2.3.1 Classe 2

Les équipements doivent être capables de contrôler l'état des accès contrôlés conformément aux règles préétablies définies par le système ou configurables. Si les règles préétablies devaient être définies par le système, le temps d'ouverture admis des accès contrôlés ne doit pas être inférieur à 10 s.

6.2.3.2 Classe 3 et classe 4

Les équipements doivent être capables de contrôler l'état des accès contrôlés et le temps d'ouverture admis de ces derniers doit être conforme aux règles préétablies configurables.

Tableau 2 – Exigences concernant les interfaces de points d'accès *(1 de 2)*

Exigences concernant les interfaces de points d'accès		Attribution de classes			
		1	2	3	4
	A – Synchronisation de libération				
1	Le temps de libération doit être défini par le système	OP*	OP*	NP	NP
2	Le temps de libération doit être configurable par accès contrôlé	OP*	OP*	M	M
3	Lorsque le temps de libération est défini par le système, la valeur admise ne doit pas être inférieure à 3 s	M	M	N/A	N/A
4	Lorsque le temps de libération est configurable, plusieurs valeurs admises peuvent être associées aux droits d'accès par accès contrôlé	OP	OP	OP	OP
	B – Contrôle d'accès				
5	Prévoir un contrôle d'accès pour l'entrée dans une zone protégée (contrôlée)	M	M	M	M
6	Prévoir un contrôle d'accès pour la sortie d'une zone protégée (contrôlée)	OP	M	M	M
7	Anti retour rigide	OP	OP	M	M
8	Anti retour souple	OP	OP	OP	OP
9	Anti retour général	OP	OP	OP	M
10	Neutralisation/désactivation du dispositif anti retour	OP	OP	OP	M
11	Anti retour temporisé	OP	OP	OP	M
12	Accès autorisé subordonné à la date d'entrée en vigueur / de fin de validité	OP	OP	M	M
13	Accès autorisé subordonné à la validité des identifiants (bloqués, suspendus, non valides)	M	M	M	M
14	Accès avec escorte des visiteurs	OP	OP	OP	OP
15	Mode de surveillance	OP	OP	OP	OP
16	Occupation double (contrôle de la présence de deux personnes ou plus)	OP	OP	OP	OP
17	Double accès (accès de deux personnes)	OP	OP	OP	M
18	Singularisation/ anti-passage en double	OP	OP	OP	OP
19	Commande de manœuvre	OP	OP	OP	OP
	C – Contrôle de l'état des points d'accès				
20	L'état des points d'accès doit être contrôlé	OP	M	M	M
21	Le temps d'ouverture admis des points d'accès doit être défini par le système (temps d'ouverture recommandé ne devant pas être inférieur à 10 s)	OP	OP*	NP	NP
22	Le temps d'ouverture des points d'accès doit être configurable par accès contrôlé	OP	OP*	M	M
23	Lorsque le temps d'ouverture est configurable, plusieurs temps d'ouverture admis peuvent être associés aux droits d'accès par point d'accès	OP	OP	OP	OP

Tableau 2 *(2 de 2)*

	Exigences concernant les interfaces de points d'accès	Attribution de classes			
		1	2	3	4
	D – Signaux d'entrée				
24	Les signaux d'entrée numériques (c'est-à-dire autres que les signaux de communication) avec une période active supérieure à 400 ms doivent être traités.	OP	M	M	M

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

NP = non permis

OP = facultatif

M = obligatoire

OP* = une des options du regroupement identifié (zone grisée) doit être mise en œuvre

N/A = non applicable

6.3 Exigences concernant l'indication et l'annonce (affichage, alerte, enregistrement)

6.3.1 Annonce

Les systèmes de contrôle d'accès électronique comprenant une console de commande doivent être capables d'afficher, signaler par alerte et enregistrer les changements au niveau de la console de commande, conformément à 6.3.1, deuxième alinéa, à 6.3.4, deuxième alinéa.

Les informations fournies conformément à 6.3.1 doivent inclure le type d'événement, son emplacement, ainsi que l'heure et la date d'occurrence.

6.3.2 Affichage

Les systèmes de contrôle d'accès électronique doivent être capables de contrôler et afficher les événements et les informations au niveau de la console de commande conformément au Tableau 3.

L'indication des informations au niveau de l'accès contrôlé doit être conforme aux exigences spécifiées dans le Tableau 3.

6.3.3 Alerte

Les systèmes de contrôle d'accès électronique doivent être capables d'activer les indicateurs au niveau de la console de commande afin de guider l'évaluation des événements par l'opérateur conformément au Tableau 3.

Les systèmes de contrôle d'accès électronique doivent être conçus de manière à traiter les signaux d'alerte conformément au Tableau 3.

6.3.4 Enregistrement

Les systèmes de contrôle d'accès électronique doivent enregistrer les événements et les informations conformément au Tableau 3.

L'accès aux informations enregistrées doit être limité par les droits de l'opérateur.

Tableau 3 – Exigences concernant l'indication et l'annonce *(1 de 4)*

Exigences concernant l'indication et l'annonce		Indication			Attribution de classes			
					1	2	3	4
A – Accès contrôlé (Indication locale)								
1	Indication visuelle et/ou sonore requise lorsque l'accès est autorisé	•			M	M	M	M
2	Indication visuelle et/ou sonore requise lorsque l'accès est refusé	•			M	M	M	M
3	Indication visuelle et/ou sonore de l'état verrouillé de l'accès contrôlé jusqu'à ce que l'accès soit autorisé	•			OP	OP	OP	OP
4	L'indication visuelle et/ou sonore est requise pour la dernière période (temps de pré-alerte) du temps d'ouverture maximal autorisé de l'accès contrôlé lorsque ce dernier reste ouvert, afin d'avertir le ou les utilisateurs du délai d'expiration du temps d'ouverture de l'accès contrôlé. Interrompre lorsque l'accès contrôlé est fermé. Le temps de pré-alerte doit être défini par l'ensemble du système ou configurable accès contrôlé par accès contrôlé (temps par défaut recommandé: 10 secondes)	•			OP	OP	M	M
B – Console de commande (annonce)								
		Affichage	Alerte	Enregistrement				
5	Une annonce visuelle est requise lorsque l'accès est autorisé	•			OP	OP	OP	OP
6	Un enregistrement est requis lorsque l'accès est autorisé			•	OP	OP	M	M
7	L'annonce visuelle, l'alerte et l'enregistrement sont requis pour les conditions d'agression	•	•	•	OP	OP	OP	M
8	Compteur d'utilisation de carte	•		•	OP	OP	OP	OP
9	L'annonce visuelle, l'alerte et l'enregistrement sont requis pour un refus d'accès en raison d'une tentative d'utilisation d'un jeton dont la validité est expirée	•	•	•	OP	OP	OP	M
10	L'annonce visuelle, l'alerte et l'enregistrement sont requis pour un refus d'accès en raison d'un nombre configurable de tentatives d'utilisation d'un jeton valide dont les informations mémorisées ne sont pas valides. Lorsque le nombre de tentatives n'est pas configurable, il doit être limité à 5	•	•	•	OP	OP	OP	M
11	L'annonce visuelle, l'alerte et l'enregistrement sont requis pour un refus d'accès en raison d'un nombre configurable de tentatives séquentielles d'utilisation d'informations mémorisées non valides (par exemple l'utilisation du code PIN uniquement pour reconnaissance). Lorsque le nombre de tentatives n'est pas configurable, il doit être limité à 5 tentatives ultérieures dans un délai de 30 s chacune	•	•	•	OP	OP	NP	NP

Tableau 3 *(2 de 4)*

Exigences concernant l'indication et l'annonce		Indication			Attribution de classes			
					1	2	3	4
B – Console de commande (annonce)								
		Affichage	Alerte	Enregistrement				
12	Indication visuelle des alertes des points d'accès sur le plan d'implantation des zones contrôlées	•			OP	OP	OP	M
13	Des instructions doivent être affichées suite aux alertes	•			OP	OP	OP	M
14	Transactions			•	OP	M	M	M
15	Annonce visuelle et enregistrement de l'état d'ouverture de l'accès contrôlé suite à l'autorisation d'accès. Peut être configurable par accès contrôlé conformément à l'exigence de classe	•		•	OP	OP	M	M
16	Annonce visuelle, alerte et enregistrement de l'état de maintien en position de fermeture de l'accès contrôlé suite à l'autorisation d'accès. Peut être configurable par accès contrôlé conformément à l'exigence de classe	•	•	•	OP	OP	OP	M
17	Accès refusé. Peut être configurable par accès contrôlé conformément à l'exigence de classe	•	•	•	OP	OP	M	M
18	Cause de refus d'accès. Peut être configurable par accès contrôlé et/ou cause de refus conformément à l'exigence de classe	•	•	•	OP	OP	OP	M
19	Changement d'état programmé ou manuel du accès contrôlé			•	OP	OP	M	M
20	Interruption de l'alimentation principale	•	•	•	OP	OP	M	M
21	Rétablissement de l'alimentation principale	•		•	OP	OP	M	M
22	Condition de dysfonctionnement de l'alimentation de secours (faible niveau de tension de batterie et absence de batterie).	•	•	•	OP	OP	M	M
23	Entrée et sortie du mode de configuration	•		•	OP	OP	M	M
24	Perte de communication entre l'unité de contrôle d'accès et la console de commande	•	•	•	OP	M	M	M
25	Appel nominal	•		•	OP	OP	M	M
26	Accès contrôlé fermé suite à ouverture forcée de l'accès contrôlé ou temps d'ouverture trop long de l'accès contrôlé	•		•	OP	OP	M	M
27	Tous les événements doivent être identifiés par type, emplacement, heure et date d'occurrence	•		•	OP	OP	M	M
28	Les alertes doivent contenir une indication de leur niveau de priorité respectif si le système autorise l'attribution de ces niveaux de priorité	•		•	OP	OP	M	M
29	Les alertes concourantes doivent être affichées par ordre de priorité lorsque le système autorise l'attribution de ces niveaux de priorité	•			OP	OP	M	M

Tableau 3 *(3 de 4)*

Exigences concernant l'indication et l'annonce		Indication			Attribution de classes			
					1	2	3	4
B – Console de commande (annonce)								
		Affichage	Alerte	Enregistrement				
30	Détection de violation	•	•	•	OP	M	M	M
31	Ouverture forcée d'un accès contrôlé	•	•	•	OP	M	M	M
32	Annonce visuelle, alerte et enregistrement pour l'expiration du temps d'ouverture admis de l'accès contrôlé (temps d'ouverture trop long de l'accès contrôlé)	•	•	•	OP	M	M	M
33	Suivi de carte	•		•	OP	OP	OP	M
34	Suivi de lecteur	•		•	OP	OP	OP	M
35	Etat du lecteur hors tension	•	•	•	OP	OP	OP	M
36	Etat anormal du dispositif de verrouillage	•	•	•	OP	OP	OP	M
37	Annonce d'atteinte d'une limite de 90 % par rapport à la capacité maximale d'enregistrement	•	•	•	OP	OP	M	M
38	Temps maximum nécessaire aux signaux pour atteindre la console de commande (90 s, 45 s et 15 s)	•	•	•	OP	90 s	45 s	15 s
39	Temps maximum d'affichage des instructions texte suite à l'alerte parvenue à la console de commande (5 s)	•	•		OP	OP	OP	M
40	Temps maximum d'affichage des images et graphiques suite à l'alerte parvenue à la console de commande (6 s)	•	•		OP	OP	OP	6 s
41	Le système doit être capable d'attribuer des niveaux de priorité aux événements d'alerte spécifiques	•			OP	OP	M	M
42	Les alertes parvenues à la console de commande requièrent l'acquittement de l'opérateur	•	•	•	OP	OP	M	M
43	L'annonce visuelle, l'alerte et l'enregistrement sont requis lorsque les conditions d'occupation double/multiple ne sont pas respectées (nombre minimum de personnes non présentes)	•	•	•	OP	OP	OP	OP
44	Tous les changements initiés par l'opérateur doivent être enregistrés avec le type, l'identifiant de l'opérateur, l'heure et la date d'occurrence			•	OP	OP	OP	M
45	Les commentaires de l'opérateur concernant les alertes doivent être enregistrés avec l'identifiant de l'opérateur, l'heure et la date de saisie du commentaire. L'alerte spécifique couverte par les commentaires doit être identifiée	•		•	OP	OP	OP	M
46	L'accès aux informations enregistrées en vue de la récupération (par exemple, affichage, impression, exportation) des événements doit être enregistré avec l'identifiant de l'opérateur, l'heure et la date d'occurrence			•	OP	OP	M	M

Tableau 3 *(4 de 4)*

Exigences concernant l'indication et l'annonce		Indication			Attribution de classes			
					1	**2**	**3**	**4**
47	Capacité d'enregistrement moyenne par lecteur du nombre minimum d'événements système			•	OP	200	500	1 000

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

NP = non permis

OP = facultatif

M = obligatoire

OP* = une des options du regroupement identifié (zone grisée) doit être mise en œuvre

N/A = non applicable

6.4 Exigences concernant la reconnaissance

Le contrôle d'accès est une application individuelle humaine qui octroie des droits d'accès à des utilisateurs individuels ou à un groupe d'utilisateurs. La reconnaissance correcte des utilisateurs est la fonction principale du système de contrôle d'accès électronique, et le choix des identifiants des utilisateurs doit par conséquent être conforme à la classe (niveau de sécurité) souhaitée:

1) les systèmes de contrôle d'accès électronique doivent permettre une reconnaissance conformément au Tableau 4;
2) les systèmes de contrôle d'accès électronique doivent comparer chaque information mémorisée avec les identifiants mémorisés, afin d'accepter ou de refuser la revendication d'identité des utilisateurs;
3) l'unité de contrôle d'accès doit comporter une horloge en temps réel ayant une précision de ±10 s par semaine et capable de s'adapter à l'heure d'été et aux années bissextiles, ainsi que de gérer les fuseaux horaires nationaux comme indiqué dans le Tableau 4. De plus, lorsque des unités de contrôle d'accès multiple sont utilisées, les horloges adaptées aux équipements de classes 3 et 4 doivent être synchronisées avec l'horloge maîtresse au moins une fois par tranche de 24 h;
4) une unité de contrôle d'accès électronique des classes 2, 3 et 4 doit fournir une identité unique à chaque utilisateur autorisé;
5) les unités de contrôle d'accès doivent fournir un nombre minimum de niveaux d'accès utilisateur selon le Tableau 4;
6) les unités de contrôle d'accès doivent fournir un nombre minimum de périodes programmables par le système selon le Tableau 4;
7) la résolution temporelle doit inclure le jour de la semaine, ainsi que l'heure et les minutes de la journée/nuit;
8) outre le point 7) ci-dessus, la résolution temporelle applicable aux équipements de classes 3 et 4 doit inclure le jour du mois, le mois et l'année;
9) les unités de contrôle d'accès doivent fournir un nombre minimum de congés et jours fériés programmables par le système selon le Tableau 4.

Tableau 4 – Exigences concernant la reconnaissance *(1 de 2)*

	Exigences concernant la reconnaissance	Attribution de classes			
		1	**2**	**3**	**4**
	A – Niveaux d'accès				
1	L'horloge en temps réel intégrée doit avoir une précision de ±10 secondes / semaine et être capable de s'adapter à l'heure d'été et aux années bissextiles	OP	M	M	M
2	Le système doit être capable de gérer plusieurs zones de temps (fuseaux horaires)	OP	OP	OP	OP
3	Pour les systèmes comportant plusieurs unités de contrôle interconnectées, les horloges doivent être synchronisées avec l'horloge maîtresse ou toute autre source de synchronisation fiable, au moins une fois par tranche de 24 h	OP	OP	M	M
4	Synchroniser l'horloge maîtresse du système sur l'heure officielle	OP	OP	OP	M
5	L'horloge en temps réel doit être maintenue pendant la période minimale indiquée en cas de perte totale d'alimentation (sauf pour la perte d'alimentation totale de la batterie de rétention des données)	OP	24 h	120 h	120 h
6	Nombre minimum de niveaux d'accès utilisateur	1	8	16	64
7	Nombre minimum de périodes configurables	0	4	8	16
8	La résolution temporelle minimale d'un niveau d'accès inclut le jour de la semaine, ainsi que les heures et minutes de la journée/nuit	N/A	M	M	M
9	La résolution temporelle minimale d'un niveau d'accès inclut le jour du mois, le mois et l'année	N/A	OP	OP	M
10	Le système doit être capable de traiter un certain nombre de jours configurables (par exemple, jours fériés, jours ouvrables et jours ouvrés particuliers)	N/A	2	16	24
11	Il convient que le système soit capable d'octroyer des droits d'accès à un groupe d'identifiants	OP	OP	OP	OP
	B – Equipements et méthodes de reconnaissance				
12	Il convient que le système soit capable de modifier les droits d'accès à un groupe d'identifiants en réponse à des circonstances exceptionnelles	OP	OP	OP	OP
13	Le système doit attribuer une identité unique à chaque utilisateur autorisé	OP	M	M	M
14	Le système doit utiliser uniquement les informations mémorisées	OP*	OP*	NP	NP
15	Le système doit utiliser la biométrie seule ou combinée à d'autres méthodes de reconnaissance	OP*	OP*	OP*	OP*
16	Le système doit utiliser un jeton	OP*	OP*	OP*	OP*
17	Le système doit utiliser les informations mémorisées et un jeton	OP*	OP*	OP*	OP*
18	L'accès doit être refusé après chaque tentative d'obtention d'un accès au moyen d'un jeton valide, avec des informations mémorisées non valides, et après un nombre prédéterminé de tentatives infructueuses, les droits d'accès applicables à ce jeton doivent être suspendus pendant une durée prédéfinie. Il est possible de configurer le nombre de tentatives. Lorsque ce nombre ne peut être configuré, il doit être limité à 5	OP	M	M	M

Tableau 4 *(2 de 2)*

Exigences concernant la reconnaissance		Attribution de classes			
		1	2	3	4
19	L'accès doit être refusé après chaque tentative d'obtention d'un accès avec des informations mémorisées non valides uniquement. L'accès doit être suspendu après 5 saisies incorrectes séquentielles dans une période prédéfinie	OP	OP	N/A	N/A
20	Lorsqu'il est fait appel à la biométrie, FAR_{ef} ne doit pas dépasser les limites indiquées pour chaque classe. NOTE 1 $FAR_{ef} = FAR$ (taux supportable d'erreur) en cas de comparaison 1:1 (par exemple, vérification biométrique d'une identité revendiquée par les informations mémorisées ou le jeton) ou $FAR_{ef} = FAR \times n$ en cas de comparaison 1:n et n = nombre de modèles mémorisés (par exemple, identification biométrique sans recourir à des informations mémorisées ou à un jeton) NOTE 2 Les valeurs FAR doivent être fondées sur la revue de la documentation fournie par le fabricant.	1 %	0,3 %	0,3 %	0,1 %
21	Le rapport minimum entre le nombre potentiel de codes utilisateur et le nombre de codes attribués doit être au moins de 1 000 pour 1 lorsque le système utilise la reconnaissance d'un utilisateur valide par les informations mémorisées uniquement par exemple: jusqu'à 10 utilisateurs – 4 chiffres, jusqu'à 100 utilisateurs – 5 chiffres, jusqu'à 1 000 utilisateurs – 6 chiffres, etc.	M	M	N/A	N/A
22	Pour les systèmes qui utilisent la reconnaissance par les informations mémorisées combinées à un jeton ou à la biométrie, ces informations mémorisées requièrent 4 chiffres au minimum	OP	OP	M	M
23	En mode de fonctionnement normal, le système doit utiliser des informations de jeton complètes (code d'installation et numéro de carte ou numéro de carte unique) à des fins de reconnaissance	M	M	M	M
24	Prise en charge de plusieurs codes d'installation si le système utilise le codage d'installation	OP	OP	OP	M
25	En mode de fonctionnement dégradé, le système peut utiliser des informations de jeton partielles (par exemple, code d'installation uniquement) à des fins de reconnaissance	OP	OP	OP	NP
26	Les jetons avec une structure de système de codage visible à l'œil nu ne doivent pas être utilisés	M	M	M	M
27	Numéro d'identité du jeton lisible sur le jeton, n'est pas une représentation directe du codage entier	M	M	M	M

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

NP = non permis

OP = facultatif

OP* = une des options du regroupement identifié (zone grisée) doit être mise en œuvre. Se reporter également aux exigences du jeton supplémentaire pour chaque classe en conformité avec le point 9) de 6.8

M = obligatoire

NA = non applicable

6.5 Exigences concernant le signalement d'agression

Le fonctionnement du dispositif de déclenchement d'agression dans la zone protégée et la transmission d'une alerte à la console de commande doivent être conformes au Tableau 5.

1) Le signal d'agression reçu à la console de commande doit comporter l'identification de l'emplacement, de l'heure et de la date.
2) Le signal d'agression reçu à la console de commande doit comporter l'identification de l'utilisateur.

Tableau 5 – Exigences concernant le signalement d'agression

Exigences concernant le signalement d'agression		Attribution de classes			
		1	2	3	4
1	L'activation de la fonctionnalité d'agression doit être configurable	OP	OP	OP	M
2	L'alerte de signalement d'agression à la console de commande doit être distincte des autres alertes	M*	M*	M*	M
3	Le fonctionnement du dispositif de déclenchement d'agression ne doit pas produire de signal potentiellement sonore ou visible sur le lieu de déclenchement de l'agression	M*	M*	M*	M

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

OP = facultatif

M = obligatoire

M* = obligatoire uniquement si la fonctionnalité facultative est prise en charge pour la classe spécifiée

6.6 Exigences concernant la neutralisation

Les systèmes de contrôle d'accès électronique doivent autoriser les commandes manuelles qui neutralisent le mode de fonctionnement configuré des points d'accès (libérer/protéger/bloquer) conformément au Tableau 6 et aux exigences ci-dessous.

1) Toutes les commandes de neutralisation doivent être enregistrées avec l'heure et la date d'occurrence.
2) Les informations enregistrées doivent inclure le type de commande de neutralisation et l'identifiant de l'opérateur.

Tableau 6 – Exigences concernant la neutralisation

Exigences concernant la neutralisation		Attribution de classes			
		1	2	3	4
1	Autorisation unique de libre accès, accès contrôlé unique	OP	OP	M	M
2	Autorisation de libre accès dans l'ensemble du système	OP	OP	OP	OP
3	Autorisation de libre accès jusqu'à une autre commande système, accès contrôlé unique ou groupe d'accès contrôlés	OP	OP	OP	OP
4	Autorisation de libre accès programmé / temporisé, accès contrôlé unique ou groupe d'accès contrôlés	OP	OP	OP	OP
5	Le système de contrôle d'accès électronique ne doit pas interdire la libre sortie autorisée par d'autres systèmes de secours (par exemple, incendie, conditions d'environnement)	M	M	M	M
6	Blocage de l'accès contrôlé jusqu'à une autre commande système, accès contrôlé unique ou groupe d'accès contrôlés	OP	OP	OP	OP
7	Blocage de l'accès contrôlé programmé / temporisé, accès contrôlé unique ou groupe d'accès contrôlés	N/A	OP	OP	OP

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

OP = facultatif

M = obligatoire

M* = obligatoire uniquement si la fonctionnalité facultative est prise en charge pour la classe spécifiée

N/A = non applicable

6.7 Exigences concernant la communication

La voie de communication entre le système de contrôle d'accès électronique et la console de commande doit satisfaire aux exigences suivantes.

1) La défaillance et/ou restauration de la voie de communication pour les équipements des classes 2, 3 et 4 ne doivent pas générer la libération des accès contrôlés.
2) La vérification de communication de bout en bout (synchronisation) doit être effectuée comme partie intégrante de l'installation finale et doit satisfaire aux exigences du Tableau 3, ligne 38, pour cette même installation.
3) Les équipements des classes 2, 3 et 4 doivent être capables de fonctionner en mode autonome après interruption de la communication avec le pupitre de contrôle. Les équipements doivent être capables d'exécuter toutes les fonctionnalités, à l'exception de celles affectées par la perte de communication.
4) Les équipements de classe 4 doivent assurer l'intégrité des communications entre tous les composants du système de contrôle d'accès qui transmettent ou reçoivent des données relatives à l'autorisation d'accès, y compris, par exemple: les communications entre les jetons/cartes et les interfaces utilisateur, les interfaces utilisateur et les unités de contrôle d'accès, et entre ces unités et le pupitre de contrôle.
5) L'intégrité de la communication doit être réalisée par la surveillance de la voie de communication (Tableau 7, ligne 9) et la sécurité des informations transmises.
6) La sécurité des informations doit être assurée par des mesures qui visent à empêcher toute lecture et toute modification non autorisées des informations transmises.
7) La description des méthodes de réalisation des mesures de sécurité des informations doit être fournie lors des essais des équipements.

6.8 Exigences concernant l'autoprotection des systèmes

Les composants des systèmes de contrôle d'accès électronique doivent satisfaire aux exigences appropriées spécifiées ci-dessous dans le Tableau 7 pour chaque classe.

1) Les boîtiers des composants des systèmes de contrôle d'accès électronique doivent comporter des moyens qui empêchent tout accès aux éléments internes afin de réduire au minimum le risque de violation. Les exigences concernant l'inviolabilité peuvent varier selon la classe du système de contrôle d'accès électronique et selon la position d'un composant du système à l'intérieur ou à l'extérieur de la zone protégée.
2) Les composants situés à l'extérieur de la zone protégée doivent comporter des moyens appropriés d'inviolabilité et de détection selon le Tableau 7, lignes 5 et 6.
3) Toutes les bornes et tous les moyens de réglage mécanique et électronique doivent se situer à l'intérieur des boîtiers des composants de contrôle d'accès électronique.
4) Les conditions de circuit ouvert ou de court-circuit appliquées aux câbles reliés aux composants d'un système de contrôle d'accès installé à l'extérieur de sa zone contrôlée ou accessible de l'extérieur de cette zone, ne doivent pas entraîner le fonctionnement du dispositif d'activation des points d'accès, autorisant l'accès à la zone protégée.
5) Les boîtiers doivent être suffisamment robustes pour empêcher tout accès non détecté aux éléments internes sans dommage visible. Le boîtier de l'interface utilisateur (par exemple, lecteur, clavier numérique, etc.) doit être protégé selon un degré de protection IP4X. Il ne doit pas être possible d'autoriser l'accès par insertion d'une sonde d'acier de 1 mm à l'intérieur du boîtier. Les caractéristiques assignées IP sont détaillées dans la CEI 60529.
6) Le boîtier de l'interface utilisateur doit être protégé selon un degré de protection IK04. Un endommagement du boîtier après impact est admis sous réserve que l'accès ne puisse pas être autorisé par une manipulation des éléments internes de l'interface utilisateur. En variante, une condition d'inviolabilité doit être générée avant toute possibilité d'accès aux éléments internes. Les caractéristiques assignées IK sont détaillées dans la CEI 62262.

7) Les moyens d'accès aux éléments internes des composants d'un système de contrôle d'accès électronique doivent être robustes et protégés mécaniquement. Un accès normal doit nécessiter l'utilisation d'un outil.

8) Les interconnexions doivent être adaptées à leur objet et conçues de manière à fournir un moyen de communication fiable entre les composants d'un système de contrôle d'accès électronique. Ces interconnexions doivent être conçues de manière à réduire au minimum toute possibilité de retard, modification, remplacement ou perte des signaux.

9) Les exigences suivantes concernant le jeton et la communication entre ce dernier et l'unité de l'interface utilisateur doivent être satisfaites, outre les exigences énoncées aux Tableaux 4 et 7:

   a) pour les classes 1 et 2, pas d'exigences supplémentaires;

   b) classe 3: jeton à contact monopuce ou sans contact (RFID) avec des conditions d'accès permettant au moins de rédiger/modifier les informations ID, ainsi que la communication de données cryptées par session pour les seuls jetons RFID. Ceci est requis uniquement lorsque le jeton est utilisé comme méthode de reconnaissance unique;

   c) classe 4: jeton à contact monopuce ou sans contact (RFID) avec des conditions d'authentification et d'accès mutuels, permettant de lire, rédiger ou modifier les informations ID, ainsi que la communication de données cryptées par session pour les seuls jetons RFID.

Tableau 7 – Exigences concernant l'autoprotection des systèmes *(1 de 3)*

Exigences concernant l'autoprotection des systèmes		Attribution de classes			
		1	2	3	4
A – Prévention					
1	Les informations mémorisées (paramétrages) doivent être maintenues pendant la période minimale indiquée en cas de perte totale d'alimentation (sauf pour la perte d'alimentation totale de la batterie de rétention des données)	10 min	2 sem	2 sem	2 sem
2	Suite à une perte totale d'alimentation, un redémarrage automatique du système de contrôle d'accès est nécessaire dès le rétablissement de la source d'alimentation principale	M	M	M	M
3	Lorsqu'il n'est pas possible de restaurer la fonctionnalité totale de l'unité de contrôle d'accès (données corrompues ou perdues) suite au redémarrage automatique, une condition de dysfonctionnement doit être annoncée	M	M	M	M
4	Les moyens d'accès aux éléments internes des composants d'un système de contrôle d'accès doivent nécessiter l'utilisation d'un outil	M	M	M	M
5	L'ouverture de l'enveloppe de l'interface utilisateur destinée à être installée à l'extérieur de la zone contrôlée ou qui peut être accessible de l'extérieur de cette zone, doit entraîner une détection de violation si la manipulation des éléments internes peut générer une condition d'accès autorisé. La détection de violation doit intervenir avant que le mécanisme d'inviolabilité puisse être mis en échec	OP	M	M	M
6	Les dispositifs destinés à être installés à l'extérieur de la zone contrôlée ou qui peuvent être accessibles de l'extérieur de cette zone doivent détecter tout retrait du support de fixation si cela permet d'accéder aux éléments internes et si la manipulation de ces éléments peut entraîner une condition d'autorisation d'accès	OP	OP	M	M
7	Les enveloppes des composants de système de contrôle d'accès électronique accessibles de l'extérieur de la zone contrôlée doivent satisfaire aux caractéristiques assignées IP et IK	IP4X IK04	IP4X IK04	IP4X IK04	IP4X IK04

Tableau 7 *(2 de 3)*

Exigences concernant l'autoprotection des systèmes		Attribution de classes			
		1	**2**	**3**	**4**
8	En cas de perte de communication entre la ou les unités de contrôle et le pupitre de contrôle, il convient que l'unité de contrôle soit capable d'archiver et de transmettre par la suite un nombre minimum d'événements par accès contrôlé, sur rétablissement des communications.	N/A	OP	500	1000
9	La communication entre l'unité de contrôle et les composants du système de contrôle d'accès électronique doit être surveillée. La perte de communication pendant la durée indiquée doit engendrer une alerte à la console de commande	N/A	OP	10 min	2 min
10	L'accès logique à l'administration système, y compris la configuration, ne doit être possible qu'à l'aide d'identifiants valides (par exemple, mot de passe, jeton)	N/A	M	M	M
11	Il doit exister des niveaux d'accès distincts qui catégorisent la capacité des opérateurs à exécuter différentes fonctions dans le système. Nombre minimum de niveaux d'accès logique:	1	1	2	4
12	Le nombre minimum de caractères requis pour l'accès logique par des informations mémorisées uniquement doit être tel qu'indiqué (N=numérique/A=alphanumérique)	4N	5N	6A	8A
13	Lorsque l'accès logique par les informations mémorisées requiert des codes numériques, des chiffres à code ascendant ou descendant séquentiels et l'utilisation d'un même chiffre à plus de deux reprises ne doivent pas être admis	OP	OP	M	M
14	Utilisation d'informations mémorisées à 4 chiffres au minimum pour un accès logique, combinées à un jeton ou à la biométrie (générées par le système ou définies par l'administrateur système)	OP	OP	M	M
15	L'identifiant d'accès logique peut être attribué uniquement par l'administrateur système	OP	OP	M	M
16	Les valeurs d'accès logique prédéfinies par le fabricant doivent pouvoir être réécrites	OP	OP	M	M
17	Après une perte d'alimentation opérationnelle, le temps de rétention minimal des données pour les événements enregistrés, mémorisés sur l'unité de contrôle d'accès (en raison de la perte de communication avec le pupitre de contrôle) doit être tel qu'indiqué	OP	24 h	120 h	120 h
18	Cryptage requis pour les signaux de communication entre les composants du système de contrôle d'accès électronique lors de l'utilisation de réseaux partagés en commun (par exemple, l'Internet)	OP	OP	M	M
19	Les informations mémorisées sur le jeton doivent être protégées contre toute modification ou reproduction non autorisée	OP	OP	M	M
20	La défaillance ou la restauration de la voie de communication ne doit pas entraîner la libération d'un point d'accès	M	M	M	M
21	La défaillance de communication avec le pupitre de contrôle ne doit pas interrompre le processus décisionnel d'accès	M	M	M	M
22	Les règles de traitement mémorisées dans un lecteur de point d'accès ne doivent pas être visibles aux utilisateurs du système	M	M	M	M
23	Les indicateurs d'activation visuels ou sonores par frappe ou par clavier numérique ne doivent pas être une représentation directe des codes réels, mais doivent avoir un pas et une durée identiques.	M	M	M	M
24	La communication entre les lecteurs et les unités de contrôle d'accès doit prendre en charge le cryptage avec authentification	OP	OP	OP*	M
25	Le manuel d'utilisation doit contenir les détails des exigences d'installation concernant la protection mécanique de limitation de l'accès aux lignes de communication entre les lecteurs et l'unité de contrôle d'accès	OP	OP	OP*	OP

Tableau 7 *(3 de 3)*

Exigences concernant l'autoprotection des systèmes		Attribution de classes			
		1	2	3	4
	B – Détection et compte-rendu				
26	Le changement d'état (ouvert, fermé, violation (violation ouverte ou fermée) d'un circuit de détection à entrée numérique doit être conçu par le fabricant de manière à s'assurer que la tolérance pour chaque état d'entrée du circuit ne doit pas chevaucher un état contigu	OP	OP	M	M
27	Validation du système d'entrée des données. Le système doit annoncer toute entrée de données non valides en mode configuration à la console de commande	M	M	M	M
28	L'accès au mode configuration doit être suspendu après une période d'inactivité prédéfinie	M	M	M	M
NOTE Les abréviations utilisées dans le tableau sont les suivantes: NP = non permis OP = facultatif M = obligatoire OP* = une des options du regroupement identifié (zone grisée) doit être mise en œuvre N/A = non applicable					

6.9 Exigences concernant l'alimentation

Il est admis que l'unité de contrôle d'accès et les composants du système de contrôle d'accès électronique soient alimentés soit par une source intégrée soit par une source distincte satisfaisant aux exigences suivantes et aux exigences appropriées du Tableau 8 pour chaque classe:

1) L'alimentation doit être capable de prendre en charge le système de contrôle d'accès électronique dans toutes les conditions, y compris la recharge de la source d'alimentation de secours pendant la période spécifiée dans le Tableau 8.
2) Il est admis que la source d'alimentation soit placée dans un ou plusieurs composants du système de contrôle d'accès électronique ou dans un boîtier distinct.

Tableau 8 – Exigences concernant l'alimentation

Exigences concernant l'alimentation		Attribution de classes			
		1	2	3	4
1	L'unité de contrôle d'accès doit comporter une source d'alimentation de secours capable de faire fonctionner l'unité et ses accessoires dans des conditions de pleine charge spécifiées pendant la période indiquée. (Les conditions de charge n'incluent pas le pupitre de contrôle et les actionneurs de points d'accès)	OP	OP	2 h	4 h
2	Suite à une interruption de la source d'alimentation principale prolongée (arrêt du système) et au rétablissement de l'alimentation, les batteries rechargeables doivent être rechargées à 80 % de leur capacité assignée dans un délai de 24 heures et à 100 % de cette même capacité dans un délai de 72 heures	M	M	M	M
3	Ni la perte de la source d'alimentation principale, ni sa restauration, ne doivent altérer le fonctionnement normal du système	OP	OP	M	M
4	En cas d'utilisation d'une source d'alimentation de secours, des dispositions doivent être prises pour surveiller les conditions suivantes: bas niveau de tension et absence de batterie (une annonce commune unique pour les deux conditions est acceptable).	OP	OP	M	M
NOTE Les abréviations utilisées dans le tableau sont les suivantes: OP = facultatif M = obligatoire					

7 Exigences concernant l'environnement et la CEM (immunité)

Chaque composant d'un système de contrôle d'accès électronique est supposé fonctionner correctement dans son environnement de service, et ce pendant une durée raisonnable. Cependant, les équipements des systèmes de contrôle d'accès étant installés dans bon nombre d'environnements très différents, la pratique ne permet pas de vérifier par essai chaque aspect des conditions d'environnement envisageables les plus extrêmes, ainsi que l'immunité aux effets électromagnétiques.

Les essais et sévérités identifiés par la présente norme sont par conséquent destinés à fournir une série pratique d'essais afin de déterminer la capacité des équipements à résister aux mécanismes de défaillance les plus susceptibles d'être générés par l'environnement dans lequel ce type d'équipement est supposé être installé, c'est-à-dire, l'environnement de service normal.

Les conditions d'environnement applicables spécifiées dans le Tableau 9 doivent être réalisées conformément aux méthodes décrites dans la CEI 62599-1.

Les conditions de compatibilité électromagnétique applicables spécifiées dans le Tableau 9 doivent être réalisées conformément aux méthodes décrites dans la CEI 62599-2.

Tableau 9 – Exigences concernant l'environnement et la CEM (immunité) *(1 de 2)*

Essai de fonctionnement réduit (8.2)		Essai	Type	Classe d'environnement I	Classe d'environnement II	Classe d'environnement III	Classe d'environnement IV
1	B,D,A	Chaleur sèche	Fonctionnement	M	M	M	M
2	B,A	Chaleur sèche	Endurance	N/A	N/A	N/A	M
3	B,D,A	Froid	Fonctionnement	M	M	M	M
4	B,D,A	Chaleur humide, régime permanent	Fonctionnement	M	N/A	N/A	N/A
5	B,A	Chaleur humide, régime permanent	Endurance	M	M	M	M
6	B,D,A	Variation de température (p)	Fonctionnement	M	M	M	M
7	B,D,A	Chaleur humide, cyclique	Fonctionnement	N/A	M	M	M
8	B,A	Chaleur humide, cyclique	Endurance	N/A	N/A	M	M
9	B, C, A	Infiltration d'eau	Fonctionnement	M(p)	M(p)	M	M
10	B,A	Dioxyde de soufre ($S0_2$)	Endurance	N/A	N/A	M	M
11	B,A	Brouillard salin, cyclique	Endurance	N/A	N/A	N/A	M
12	B, C, A	Impact (f) (m)	Fonctionnement	M	M	M	M
13	B,A	Poussière	Endurance	N/A	N/A	M	M
14	B, C, A	Chute libre (m) (p)	Fonctionnement	M	M	M	M
15	B, C, A	Choc (f)	Fonctionnement	M	M	M	M
16	B, C, A	Vibrations, sinusoïdales	Fonctionnement	M	M	M	M
17	B, C, A	Variations de la tension d'alimentation de secteur	Fonctionnement	M	M	M	M
18	B, C, A	Chutes et courtes interruptions de tension d'alimentation de secteur	Fonctionnement	M	M	M	M
19	B, C, A	Décharge électrostatique	Fonctionnement	M	M	M	M

Tableau 9 *(2 de 2)*

Essai de fonctionnement réduit (8.2)		Essai	Type	Classe d'environnement I	Classe d'environnement II	Classe d'environnement III	Classe d'environnement IV
20	B, C, A	Champs électromagnétiques rayonnés	Fonctionnement	M	M	M	M
21	B, C, A	Perturbations conduites, induites par des champs électromagnétiques	Fonctionnement	M	M	M	M
22	B, C, A	Rafales transitoires rapides	Fonctionnement	M	M	M	M
23	B, C, A	Surtension à haute énergie lente	Fonctionnement	M	M	M	M

NOTE Les abréviations utilisées dans le tableau sont les suivantes:

A après une période de conditionnement et de récupération

B avant conditionnement

C contrôle en cours de conditionnement

D en cours de conditionnement, contrôle et réalisation d'un essai de fonctionnement réduit comme spécifié dans la CEI 62599-1

M obligatoire

N/A non applicable

(f) applicable à des équipements fixes

(m) applicable à des équipements mobiles

(p) applicable aux matériels portables

8 Méthodes d'essai

8.1 Conditions générales

8.1.1 Conditions atmosphériques pour essais

Sauf indication contraire dans un mode opératoire, les essais doivent être effectués après avoir laissé se stabiliser l'éprouvette dans les conditions atmosphériques normales pour les essais décrites dans la CEI 60068-1, comme suit:

– température: (15 à 35) °C;

– humidité relative: (25 à 75) %;

– pression de l'air: (86 à 106) kPa.

Lorsque les variations de ces paramètres ont un impact significatif sur une mesure, il convient alors de maintenir celles-ci à un niveau minimum au cours d'une série de mesures effectuées comme partie intégrante d'un essai effectué sur une éprouvette.

8.1.2 Conditions de fonctionnement pour essais

Lorsqu'une méthode d'essai nécessite de faire fonctionner une éprouvette, cette dernière doit être reliée à un équipement d'alimentation réglé dans la ou les plages de tensions spécifiées par le fabricant et doit rester essentiellement constante pendant la durée des essais. Lorsqu'un mode opératoire nécessite de contrôler une éprouvette afin de détecter les signaux d'alerte éventuels, des connexions doivent être établies avec les dispositifs auxiliaires nécessaires afin de pouvoir reconnaître le signal.

Tous les signaux/messages d'entrée doivent être correctement terminés selon les instructions du fabricant.

Les sorties doivent être reliées aux charges représentatives des conditions maximales relevant des spécifications du fabricant.

Tous les trajets de transmission doivent être reliés à des équipements compatibles. Tous les circuits de sortie doivent être reliés à des charges maximales, toutes ces charges relevant des spécifications du fabricant.

8.1.3 Configuration des éprouvettes

La configuration des éprouvettes doit comprendre au moins un de chaque type d'interfaces utilisateur de points d'accès compatibles/prise en charge, d'actionneurs de points d'accès ou d'indicateurs équivalents (avec des charges équivalentes), d'application de pupitre de contrôle ou équivalent (lorsque fourni), configuré par le fabricant afin d'assurer le fonctionnement dépendant de la classe, comme défini dans les Tableaux 2 à 8.

Tout équipement supplémentaire nécessaire pour effectuer les essais (par exemple: moyens de contrôle de l'état des sorties et moyens d'activation des entrées) doit être fourni par le fabricant sur accord avec le laboratoire d'essai.

Les éprouvettes soumises doivent être représentatives de la production normale du fabricant eu égard à leurs paramètres de construction et de configuration, et doivent comporter les options revendiquées.

8.1.4 Dispositions de montage

L'éprouvette doit être montée par ses moyens normaux de fixation conformément aux instructions du fabricant. Lorsque ces instructions décrivent deux méthodes de montage ou plus, la méthode considérée comme étant la moins favorable doit alors être choisie pour chaque essai.

8.1.5 Tolérances

Sauf indication contraire, les tolérances relatives aux paramètres d'essai d'environnement doivent être telles qu'indiquées dans les normes de référence de base pour l'essai (par exemple, la partie correspondante de la CEI 60068). Lorsqu'une exigence ou un mode opératoire ne spécifie aucune tolérance ou limite d'écart spécifique, une limite d'écart de ±5 % doit alors être appliquée.

8.1.6 Dispositions pour essais

Un système de contrôle d'accès au moins doit être prévu pour vérifier par essai la conformité avec la présente partie de la CEI 60839. Les éprouvettes soumises doivent être représentatives de la production normale du fabricant eu égard à leur construction et à leurs paramètres, et doivent comporter les options revendiquées.

Les exigences énumérées de 6.2 à 6.9 doivent être vérifiées par essai en utilisant le système/les composants de contrôle d'accès connectés conformément au système donné en

exemple à la Figure 3 (ou à une partie de ce dernier selon ce qui est considéré applicable) et en utilisant les fonctions configurées par le fabricant afin d'assurer le fonctionnement dépendant de la classe comme défini dans les Tableaux 2 à 8.

Lorsque les composants individuels sont évalués selon la présente norme, par exemple, un lecteur, les essais doivent être effectués avec le composant concerné connecté à un système de contrôle d'accès configuré pour au minimum prendre en charge le fonctionnement de ce même composant. En variante, il est admis de soumettre à essai les composants individuels en simulant les fonctions d'un système de contrôle d'accès, sous réserve d'un accord entre le demandeur et le laboratoire d'essai stipulant que la méthode de simulation permet de vérifier la fonctionnalité applicable pour le composant respectif.

Les composants de systèmes de contrôle d'accès électronique ayant plusieurs fonctionnalités décrites à l'Article 6 doivent être évalués en choisissant les essais pertinents décrits dans l'Article 8 pour la classe appropriée. Le laboratoire d'essai est chargé de procéder à ce choix conformément aux fonctionnalités et aux caractéristiques assignées de classe revendiquées par le fabricant.

8.1.7 Fonctions facultatives

La présente partie de la CEI 60839 spécifie les fonctionnalités obligatoires et facultatives. Une unité ou un composant de contrôle d'accès d'un système de même nature conforme à la présente partie de la CEI 60839, est tenu(e) de satisfaire aux exigences de toutes les fonctions obligatoires.

Si une fonction fournie est facultative pour une classe particulière et si la conformité est revendiquée, cette fonction doit satisfaire aux exigences applicables concernant la classe pour laquelle la conformité est revendiquée, et elle doit par ailleurs être soumise à essai.

Les fonctionnalités complémentaires aux fonctionnalités obligatoires spécifiées dans la présente norme peuvent être intégrées au système de contrôle d'accès électronique, à condition qu'elles n'empêchent pas le fonctionnement correct des fonctionnalités obligatoires.

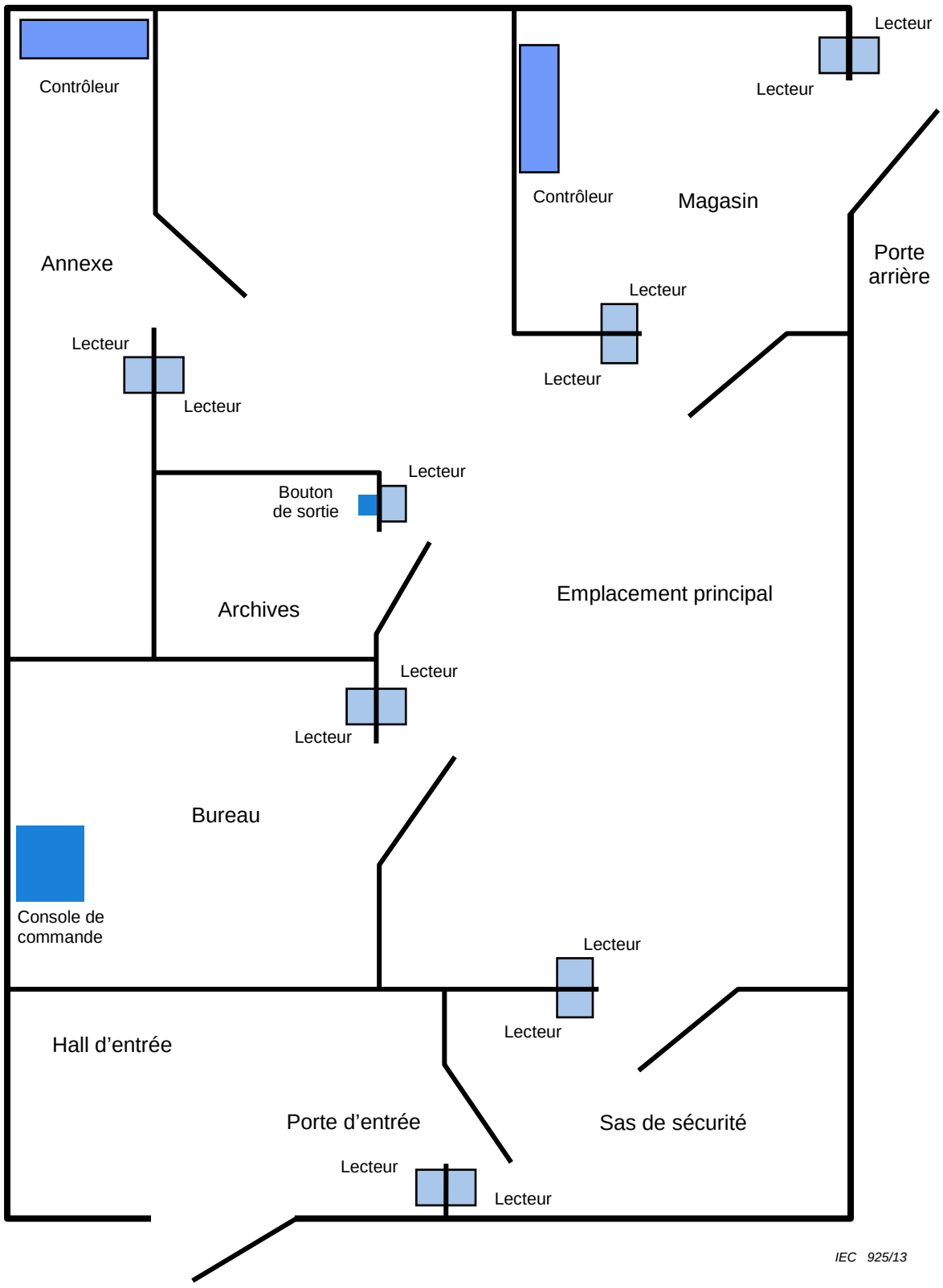


Figure 3 – Exemple de configuration d'essai de système

8.2 Essai de fonctionnement réduit

Pour les exemples, (par exemple: essais d'environnement, essais CEM), il peut arriver que l'on ne puisse pas ou qu'il ne soit pas souhaitable d'effectuer un essai de fonctionnement intégral. Dans ces cas, un essai de fonctionnement réduit doit être effectué conformément au mode opératoire ci-dessous:

1) Présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès et simuler l'ouverture et la fermeture de l'accès contrôlé.
2) Consigner la réponse des sorties d'annonce au point d'accès et confirmer que la fonctionnalité est conforme au Tableau 3, ligne 1.
3) Confirmer par inspection que l'indication de l'état de fermeture du point d'accès fait l'objet d'un affichage jusqu'à ce qu'un accès soit autorisé, et jusqu'à ce que la fonctionnalité soit conforme au Tableau 3, ligne 3.
4) Présenter des identifiants non valides à un point d'accès afin de créer une condition de refus d'accès et consigner la réponse des sorties d'annonce, puis vérifier que la raison du refus d'accès figure dans le journal des événements.
5) Confirmer que la fonctionnalité est conforme au Tableau 3, lignes 2, 17 et 18.
6) Présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès et simuler l'ouverture de l'accès contrôlé. Maintenir l'accès contrôlé ouvert jusqu'au terme du délai d'expiration du temps d'ouverture admise et confirmer la génération d'une alerte.
7) Confirmer que la fonctionnalité est conforme au Tableau 3, lignes 4 et 32.
8) Fermer l'accès contrôlé et confirmer que la fonctionnalité est conforme au Tableau 3, lignes 4 et 26.

8.3 Essais de fonctionnement pour une interface de points d'accès

8.3.1 Objet de l'essai

Démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences de 6.2 et du Tableau 2.

8.3.2 Principe

Le système de contrôle d'accès décrit à la Figure 3 doit être utilisé pour démontrer les fonctions dépendant de la classification de sécurité, énumérées dans les exigences indiquées dans le Tableau 2. Présenter les identifiants programmés (codes, cartes, etc.) au point d'accès et s'assurer du traitement de la saisie dans la période requise, ainsi que de l'indication et de la(des) notification(s) correcte(s) effective(s) (voir Tableau 2). Le laboratoire doit vérifier la documentation fournie par le fabricant, pour la prise en charge des fonctionnalités obligatoires et facultatives décrites dans le Tableau 2 pour la classe attribuée à l'unité de contrôle d'accès.

8.3.3 Procédure

8.3.3.1 Interface de points d'accès – Synchronisation de libération (réf. Tableau 2, lignes 1 à 4)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 2, lignes 1 à 4, suivre les étapes suivantes:

1) Le système doit être programmé pour une information d'utilisateur valide (identifiant), dans des conditions normales.
2) Vérifier la documentation fournie par le fabricant et déterminer si le temps de libération est défini par le système ou configurable pour chaque point (accès contrôlé) d'accès.
3) Saisir les informations d'utilisateur, l'accès doit alors être autorisé.

4) Mesurer le temps de libération et consigner le résultat, la fonctionnalité doit être conforme au Tableau 2, lignes 1 à 4.

8.3.3.2 Interface de points d'accès – Contrôle d'accès (réf. Tableau 2, lignes 5 à 19)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 2, lignes 5 à 19, suivre les étapes suivantes:

1) Le système doit être programmé pour une information d'utilisateur valide (identifiant), dans des conditions normales. Le système doit comporter deux points d'accès, un point étant programmé comme entrée et l'autre point étant programmé comme sortie d'une zone contrôlée.
2) Vérifier la documentation fournie par le fabricant et déterminer la mise en œuvre ou non de la règle anti retour, ainsi que les options applicables à cette règle qui sont effectivement prises en charge (rigide, souple, temporisée, générale, neutralisation/désactivation et périodes anti retour). Activer une fonction anti retour prise en charge à la fois.
3) Saisir les informations d'utilisateur au point d'accès d'entrée et vérifier l'autorisation de l'accès. La fonctionnalité doit être conforme au Tableau 2, ligne 5.
4) Saisir à nouveau les mêmes informations d'utilisateur au point d'accès d'entrée (avant et après la période anti retour programmée) et consigner le résultat.
5) Saisir les informations d'utilisateur au point d'accès de sortie et vérifier l'autorisation de l'accès. La fonctionnalité doit être conforme au Tableau 2, ligne 6.
6) Saisir à nouveau les mêmes informations d'utilisateur au point d'accès de sortie (avant et après la période anti retour programmée) et consigner le résultat.
7) Répéter l'essai pour chaque option anti retour prise en charge par le système de contrôle d'accès.
8) La fonctionnalité relative aux options anti retour prises en charge doit être conforme au Tableau 2, lignes 7 à 11.
9) Programmer une date d'entrée en vigueur/de fin de validité des informations d'utilisateur.
10) Saisir les informations d'utilisateur au point d'accès à compter de la date d'entrée en vigueur/avant la date de fin de validité fixées pour cet identifiant, l'accès doit alors être autorisé.
11) Saisir les informations d'utilisateur au point d'accès après la date d'entrée en vigueur/la date de fin de validité fixées pour cet identifiant, l'accès doit alors être refusé. La fonctionnalité doit être conforme au Tableau 2, lignes 12 et 13.
12) Programmer deux informations d'utilisateur ayant les mêmes niveaux d'accès.
13) Programmer un point d'accès pour qu'il autorise une saisie uniquement lorsque deux demandes d'accès autorisé séquentielles sont formulées dans une période limitée programmable. Programmer le délai admis à 2 minutes.
14) Présenter une information d'utilisateur, l'accès ne doit alors pas être autorisé.
15) Présenter les première et seconde informations d'utilisateur dans un délai de 2 minutes, l'accès doit alors être autorisé.
16) Présenter la première information d'utilisateur, attendre 2 minutes, présenter la seconde information d'utilisateur, l'accès ne doit alors pas être autorisé. La fonctionnalité doit être conforme au Tableau 2, ligne 17.

8.3.3.3 Interface de points d'accès – Contrôle de l'état des points d'accès (réf. Tableau 2, lignes 20 à 23)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 2, lignes 20 à 23, suivre les étapes suivantes:

1) Le système doit être programmé pour une information d'utilisateur valide (identifiant), dans des conditions normales.

2) Vérifier la documentation fournie par le fabricant et déterminer si le temps d'ouverture du point d'accès est défini par le système et programmable pour chaque point/accès contrôlé d'accès.

3) Saisir les informations d'utilisateur, l'accès doit alors être autorisé.

4) Mesurer le temps d'ouverture de l'accès contrôlé et consigner le résultat. La fonctionnalité doit être conforme au Tableau 2 lignes, 20 à 22.

8.3.3.4 Interface de points d'accès – Traitement des signaux d'entrée (réf. Tableau 2, ligne 24)

Appliquer un signal d'entrée (par exemple, violation) avec une durée active minimale de 400 ms et consigner l'annonce éventuelle de l'événement à la console de commande. La fonctionnalité doit être conforme au Tableau 2, ligne 24.

8.3.4 Critères de conformité

L'état d'activation et de contrôle des points d'accès doit être conforme aux exigences dépendant de la classification de sécurité indiquées dans le Tableau 2.

8.4 Essais de fonctionnement pour l'indication/annonce (affichage, alerte et enregistrement)

8.4.1 Objet de l'essai

Démontrer par inspection et essai que le système de contrôle d'accès peut satisfaire aux fonctionnalités d'indication/annonce du 6.3 et du Tableau 3.

8.4.2 Principes

Le système de contrôle d'accès décrit à la Figure 3 doit être utilisé pour démontrer les fonctions dépendant de la classification de sécurité d'affichage, alerte et enregistrement énumérées dans les exigences indiquées dans le Tableau 3.

8.4.3 Mode opératoire

8.4.3.1 Indications d'accès contrôlés (réf. Tableau 3, lignes 1 à 4) et annonce à la console de commande (réf. Tableau 3 lignes 17, 18, 26 et 32)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 3, lignes 17, 18, 26 et 32, suivre les étapes suivantes:

1) Lorsque l'option existe, vérifier qu'une indication de l'état de fermeture de l'accès contrôlé s'affiche jusqu'à l'autorisation d'accès. La fonctionnalité doit être conforme au Tableau 3, ligne 3.

2) Présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès. Consigner la réponse des sorties d'annonce à l'accès contrôlé. La fonctionnalité doit être conforme au Tableau 3, ligne 1.

3) Présenter des identifiants non valides à un point d'accès afin de créer une condition de refus d'accès et consigner la réponse des sorties d'annonce. S'assurer que la raison du refus d'accès figure dans le journal des événements. La fonctionnalité doit être conforme au Tableau 3, lignes 2 et 18.

4) Pour un fonctionnement conforme au système, présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès et simuler l'ouverture de l'accès contrôlé. Maintenir l'ouverture de l'accès contrôlé jusqu'à ce que le temps de pré-alerte défini par le système commence et consigner la réponse des sorties d'annonce à l'accès contrôlé. Maintenir l'ouverture de l'accès contrôlé jusqu'au terme du délai d'expiration du temps d'ouverture admise défini par le système et confirmer la génération d'une alerte à la console de commande. La fonctionnalité doit être conforme au Tableau 3, lignes 4 et 32.

5) Fermer l'accès contrôlé et enregistrer le temps nécessaire à l'interruption de l'alerte. La fonctionnalité doit être conforme au Tableau 3, lignes 4 et 26.

8.4.3.2 Pupitre de contrôle (réf. Tableau 3, lignes 5 à 47)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 3, lignes 5 à 47, suivre les étapes suivantes:

1) Présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès et simuler l'ouverture et la fermeture de l'accès contrôlé. Consigner la réponse des sorties d'annonce à la console de commande. La fonctionnalité doit être conforme au Tableau 3, lignes 6, 15 et 27.
2) Lorsque l'option existe, confirmer la présence d'une annonce visuelle lorsque l'accès est autorisé. La fonctionnalité doit être conforme au Tableau 3, ligne 5.
3) Lorsque l'option existe, vérifier le fonctionnement de l'annonce du compteur d'utilisation de carte. La fonctionnalité doit être conforme au Tableau 3, ligne 8.
4) Créer une condition d'agression et consigner la réponse des sorties d'annonce à la console de commande. La fonctionnalité doit être conforme au Tableau 3, ligne 7.
5) Présenter un jeton, avec une période de validité expirée, à un point d'accès et consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, ligne 9.
6) Présenter un jeton valide, conjointement à des informations mémorisées valides (par exemple, PIN) à un point d'accès à configuration appropriée afin de créer une condition d'autorisation d'accès et simuler l'ouverture et la fermeture de l'accès contrôlé. Confirmer que le fonctionnement est correct selon le Tableau 3, lignes 1, 6, 15 et 27.
7) Présenter de manière répétée un jeton valide, conjointement à des informations mémorisées non valides (par exemple, PIN erroné) au même accès contrôlé. Contrôler la réponse des sorties d'annonce et enregistrer le nombre de tentatives jusqu'à l'indication d'une alerte. La fonctionnalité doit être conforme au Tableau 3, ligne 10.
8) Présenter des informations mémorisées valides (par exemple, PIN) à un point d'accès à configuration appropriée afin de créer une condition d'accès autorisé et simuler l'ouverture et la fermeture de l'accès contrôlé. Confirmer que le fonctionnement est correct selon le Tableau 3, lignes 1, 6, 15 et 27.
9) Présenter de manière répétée des informations mémorisées non valides (par exemple, PIN erroné) au même accès contrôlé. Contrôler la réponse des sorties d'annonce et enregistrer le nombre de tentatives jusqu'à l'indication d'une alerte. La fonctionnalité doit être conforme au Tableau 3, ligne 11.
10) Soumettre la fonctionnalité à une classification de sécurité, confirmer par inspection que le système a la possibilité d'afficher une carte de la zone contrôlée et des points d'accès pour lesquels une alerte a été générée. La fonctionnalité doit être conforme au Tableau 3, ligne 13.
11) Soumettre la fonctionnalité à une classification de sécurité, confirmer par inspection que le système a la possibilité d'afficher des instructions suite à une alerte. La fonctionnalité doit être conforme au Tableau 3, ligne 12.
12) Avec une simulation de l'accès contrôlé fermé, présenter des identifiants valides à un point d'accès afin de créer une condition d'autorisation d'accès, en maintenant toutefois l'accès contrôlé fermé, simulant une défaillance d'entrée. Consigner la réponse des sorties d'annonce à l'accès contrôlé et confirmer l'enregistrement de la transaction non aboutie dans le journal des événements, une indication d'alerte étant générée selon le Tableau 3, ligne 16.
13) Confirmer par essai que les changements apportés à l'état verrouillé/déverrouillé de l'accès contrôlé à programmation horaire et/ou manuelle (via une libération d'annulation manuelle) sont affichés et que l'événement est consigné dans le journal. La fonctionnalité doit être conforme au Tableau 3, ligne 19.

14) Retirer la source d'alimentation principale (par exemple, alimentation réseau) du système en essai. Consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, lignes 20, 27 et 28.

15) Réinitialiser la source d'alimentation principale et confirmer que l'événement est consigné dans le journal. La fonctionnalité doit être conforme au Tableau 3, ligne 21.

16) Créer une condition d'alimentation de secours de faible puissance en mettant en place soit une batterie déchargée, soit en remplaçant la source d'alimentation de secours normale par une alimentation variable, ajustée lentement de la tension de secours nominale à la condition d'alimentation de faible puissance. Consigner la réponse des sorties d'annonce une fois la condition d'alimentation de faible puissance atteinte. La fonctionnalité doit être conforme au Tableau 3, lignes 22, 27 et 28.

17) Retirer la source d'alimentation de secours une fois l'alimentation de secours normale réinitialisée et avec le système de contrôle d'accès fonctionnant normalement. Consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, lignes 22, 27 et 28.

18) Confirmer par essai l'affichage de l'entrée et de la sortie du mode de programmation et leur enregistrement dans le journal des événements. La fonctionnalité doit être conforme au Tableau 3, ligne 23.

19) Interrompre les liaisons de communication suivantes à tour de rôle, tout en contrôlant les sorties d'annonce et en mesurant la durée nécessaire à l'annonce de l'alerte:

    a) la liaison entre l'interface utilisateur des points d'accès et l'unité de contrôle d'accès;

    b) la liaison entre l'unité de contrôle d'accès et le pupitre de contrôle.

20) A l'interruption de la liaison entre l'interface utilisateur des points d'accès et l'unité de contrôle d'accès, mesurer et enregistrer le temps qui s'écoule entre le moment d'interruption et le moment d'indication de l'alerte à la console de commande. La fonctionnalité doit être conforme au Tableau 3, lignes 24, 27, 28, 35 et 38.

21) Lorsque l'option d'affichage d'instructions texte s'applique après une alerte, mesurer et enregistrer également le temps qui s'écoule entre le moment d'indication de l'alerte à la console de commande et le moment où les instructions texte associées au message d'alerte s'affichent sur ce pupitre. La fonctionnalité doit être conforme au Tableau 3, ligne 39.

22) Lorsque l'option d'affichage d'images et/ou de graphiques s'applique après une alerte, mesurer et enregistrer également le temps qui s'écoule entre le moment d'indication de l'alerte à la console de commande et le moment où les images et/ou graphiques associés au message d'alerte s'affichent sur ce pupitre. La fonctionnalité doit être conforme au Tableau 3, ligne 40.

23) Créer des alertes système au niveau des éléments hors ligne. Noter l'heure réelle et attendre au moins 5 minutes.

24) Chaque liaison de communication doit être réinitialisée et un fonctionnement correct doit être démontré entre les tentatives d'interruption. La fonctionnalité doit être conforme au Tableau 3, lignes 14 et 27.

25) Vérifier que les alertes système sont reçues dans le journal avec datations de l'occurrence effective de l'alerte, et non de la réception effective à la console de commande. La fonctionnalité doit être conforme au Tableau 3, ligne 27.

26) Présenter cinq ensembles d'identifiants valides à un ou plusieurs points d'accès à tour de rôle, en créant une condition d'autorisation d'accès et en simulant à chaque fois l'ouverture et la fermeture de l'accès contrôlé. Retirer ensuite un ensemble d'identifiants de la zone contrôlée en mettant en œuvre une procédure de sortie appropriée.

27) Contrôler et consigner la réponse des sorties d'annonce, et confirmer que:

    a) l'appel nominal du journal des événements reflète le nombre correct d'identifiants enregistrés comme se trouvant toujours "DANS" la zone contrôlée par le système. La fonctionnalité doit être conforme au Tableau 3 ligne 25;

b) les identifiants qui ont été retirés de la zone contrôlée par mise en œuvre de la procédure de sortie sont identifiés correctement, comme se trouvant à l'extérieur de ladite zone;

c) le journal des événements doit avoir enregistré l'identité du ou des lecteurs spécifiques auxquels les identifiants ont été présentés.

28) Avec le système de contrôle d'accès fonctionnant normalement, et tous les accès contrôlés étant protégés, appliquer les entrées appropriées qui permettent de simuler l'action d'une ouverture forcée, c'est-à-dire sans autorisation d'accès. Consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, ligne 31.

29) Ouvrir une enveloppe comportant un moyen de détection de violation et consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, ligne 30.

30) Simuler une condition de dispositif de verrouillage anormal par l'application du ou des signaux d'entrée appropriés et consigner la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, ligne 36.

31) En se référant à la documentation fournie par le fabricant, créer un nombre suffisant d'événements afin de remplir le journal des événements à 90 % de la capacité d'enregistrement. La fonctionnalité doit être conforme au Tableau 3, ligne 37.

32) Confirmer par essai qu'il est possible d'attribuer des priorités aux événements d'alerte spécifiques. Sélectionner de manière aléatoire au moins trois événements d'alerte configurables. La fonctionnalité doit être conforme au Tableau 3, lignes 28, 29 et 41.

33) Générer plusieurs (trois au minimum) événements d'alerte configurables comprenant des priorités spécifiques attribuées. Consigner la réponse des sorties d'annonce. Acquitter chaque événement d'alerte et consigner à nouveau la réponse des sorties d'annonce. Confirmer l'affichage des alertes dans l'ordre des priorités spécifié par le fabricant de l'unité de contrôle d'accès. La fonctionnalité doit être conforme au Tableau 3, ligne 29.

34) Faire fonctionner le système de contrôle d'accès afin de générer l'un des événements d'alerte sélectionnés. Consigner la réponse des sorties d'annonce. Acquitter l'événement d'alerte et consigner à nouveau la réponse des sorties d'annonce. La fonctionnalité doit être conforme au Tableau 3, ligne 42.

35) Lorsque l'opérateur a la possibilité d'inclure des commentaires en réponse aux alertes, confirmer également que le système génère une entrée dans le journal des événements. L'entrée doit inclure une datation (heure et date), l'événement d'alerte auquel les commentaires se rapportent et l'identité de l'opérateur. La fonctionnalité doit être conforme au Tableau 3, ligne 45.

36) Présenter cinq ensembles d'identifiants valides à un ou plusieurs points d'accès à tour de rôle, en créant une condition d'autorisation d'accès et en simulant à chaque fois l'ouverture et la fermeture de l'accès contrôlé. Retirer ensuite quatre ensembles d'identifiants de la zone contrôlée en mettant en œuvre les procédures de sortie appropriées. Contrôler et consigner la réponse de la sortie d'annonce, et confirmer l'affichage conjoint d'un avertissement associé au nombre minimum de personnes non présentes avec une alerte et une entrée dans le journal des événements. La fonctionnalité doit être conforme au Tableau 3, ligne 43.

37) Confirmer par essai que les changements initiés par l'opérateur sont consignés dans le journal des événements. La fonctionnalité doit être conforme au Tableau 3, ligne 44. L'enregistrement doit inclure les éléments suivants:

a) le type de paramètre modifié;

b) l'identification de l'opérateur;

c) la datation.

38) La création, l'impression et l'exportation des rapports de gestion doivent être vérifiées par rapport aux spécifications du fabricant. La fonctionnalité doit être conforme au Tableau 3, ligne 46.

Le rapport dédié aux systèmes de classes 3 et 4 doit comporter au minimum:

a) les détails de toutes les activités de circuit;

b) une synthèse de toutes ou d'une partie des activités de circuit sélectionnées, y compris les alarmes individuelles au cours d'une période choisie. (Par exemple, le système doit être capable de rechercher toutes les activités de circuit ou les activités d'un seul circuit au cours par exemple de la dernière heure, même en l'absence d'événements d'alarme);

c) les actions de l'opérateur relatives aux circuits et aux lecteurs au cours d'une période choisie;

d) les alarmes de contrôle d'accès;

e) l'activité du ou des lecteurs de contrôle d'accès sur une base par utilisateur;

f) les informations d'utilisateur de contrôle d'accès;

g) les informations de circuit: détail complet pour chaque point d'entrée et de sortie configuré;

h) les changements de la ou des bases de données utilisateur;

i) la disponibilité du système: un journal de toutes les parties du système, qui décrit en détail les périodes sous tension et hors tension de chaque partie individuelle;

j) les fichiers de bases de données et les configurations système.

39) Confirmer, par inspection de la documentation fournie par le fabricant, que la console de commande est en mesure de satisfaire aux exigences dépendant de la classification de sécurité pour la capacité minimale d'enregistrement des événements dans un journal du système. La fonctionnalité doit être conforme au Tableau 3, ligne 47.

40) Présenter trois identifiants valides à trois lecteurs différents. La fonctionnalité doit être conforme au Tableau 3, ligne 33.

41) Présenter trois identifiants valides différents à un lecteur et deux identifiants non valides au même lecteur. La fonctionnalité doit être conforme au Tableau 3, ligne 34.

8.4.4 Critères de conformité

L'état des sorties d'annonce doit être conforme aux exigences dépendant de la classification de sécurité indiquées dans le Tableau 3.

8.5 Méthodes d'essai pour les fonctionnalités de reconnaissance

8.5.1 Objet de l'essai

Démontrer par inspection et essai que le système de contrôle d'accès peut satisfaire aux fonctionnalités de reconnaissance de 6.4 et du Tableau 4.

8.5.2 Principes

Le système de contrôle d'accès décrit à la Figure 3 doit être utilisé pour démontrer que les fonctions de reconnaissance dépendant de la classification de sécurité s'appliquent comme énumérées dans les exigences indiquées dans le Tableau 4.

8.5.3 Mode opératoire

8.5.3.1 Niveaux d'accès (réf. Tableau 4, lignes 1 à 12)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 4, lignes 1 à 12, suivre les étapes suivantes:

1) Au début de chaque essai, régler l'horloge en temps réel sur l'heure effective. Après une journée, vérifier si l'horloge en temps réel diffère de l'heure effective d'une valeur inférieure ou égale à la valeur admise calculée selon le Tableau 4, ligne 1.

2) Régler la date de changement de l'heure normale à l'heure d'été et l'heure 2 minutes avant le changement attendu. Consigner le changement effectif ou non qui se produit

entre l'heure normale et l'heure d'été à l'heure de changement officielle, selon le Tableau 4, ligne 1.

3) Régler la date de changement de l'heure d'été à l'heure normale et l'heure 2 minutes avant le changement attendu. Consigner le changement effectif ou non qui se produit entre l'heure d'été et l'heure normale à l'heure de changement officielle, selon le Tableau 4, ligne 1.

4) Régler la date au 28 février de la prochaine année bissextile et l'heure à 23:58. Enregistrer le passage éventuel à minuit de la date au 29 février selon le Tableau 4, ligne 1.

5) Régler la date au 28 février d'une année non bissextile et l'heure à 23:58. Enregistrer le passage éventuel à minuit de la date au 1er mars selon le Tableau 4, ligne 1.

6) Régler l'horloge maîtresse sur l'heure et la date correctes. Régler l'horloge en temps réel esclave sur l'heure et la date erronées. Régler l'heure de l'horloge maîtresse sur 2 min avant le temps de synchronisation (indiqué par le fabricant). Enregistrer la synchronisation éventuelle de l'horloge en temps réel esclave sur les mêmes date et heure que l'horloge maîtresse. Confirmer, par revue de la documentation d'accompagnement, que le temps de synchronisation se répète quotidiennement (c'est-à-dire sans saisie de date). La fonctionnalité doit être conforme au Tableau 4, ligne 3.

7) Régler l'horloge maîtresse de l'unité de contrôle d'accès sur l'heure et la date erronées. Relier l'horloge maîtresse de l'EACS à l'horloge maîtresse officielle des locaux, qui donne l'heure officielle. Confirmer, après une période maximale de 15 minutes, que l'horloge maîtresse de l'EACS est synchronisée sur l'heure officielle selon le Tableau 4, ligne 4.

8) Confirmer que l'horloge en temps réel est réglée pour afficher l'heure correcte. Déconnecter l'alimentation de secteur et les batteries de secours (les batteries de rétention des données doivent rester connectées). Après les périodes définies par la classe de système appropriée, reconnecter l'alimentation de secteur et les batteries de secours. L'ordre de reconnexion doit être conforme aux recommandations du fabricant des équipements. Confirmer par inspection de l'horloge en temps réel que le système de contrôle d'accès affiche l'heure correcte. La fonctionnalité doit être conforme au Tableau 4, ligne 5.

9) Examiner la documentation fournie par le fabricant et déterminer que le nombre de niveaux d'accès de l'utilisateur et le nombre de zones de temps satisfont ou dépassent les exigences indiquées dans le Tableau 4, lignes 6 et 7.

10) Vérifier qu'il est possible de saisir le jour, la semaine, l'heure et les minutes ou la date, année, mois et jour, ou l'heure et les minutes respectivement, pour les niveaux d'accès requis par le Tableau 4, lignes 8 et 9.

11) Vérifier que le nombre donné de jours configurables (c'est-à-dire jours particuliers) est traité correctement par le système de contrôle d'accès électronique selon le Tableau 4, ligne 10.

8.5.3.2 Equipements et méthodes de reconnaissance (réf. Tableau 4, lignes 13 à 27)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 4, lignes 13 à 27, suivre les étapes suivantes:

1) Tenter d'ajouter un nouveau jeton au système comportant le même nombre de jetons déjà autorisés ou tenter d'attribuer le même jeton à deux utilisateurs. Confirmer le rejet de cette tentative. La fonctionnalité doit être conforme au Tableau 4, ligne 13.

2) Régler l'EACS en fonctionnement, en n'attribuant aucun niveau d'accès aux utilisateurs/détenteurs de carte. Attribuer un identifiant approprié à un utilisateur/détenteur de carte du système. Attribuer un niveau d'accès à cet utilisateur. Appliquer l'identifiant à un lecteur/clavier numérique ou capteur biométrique à la fois, au cours d'une période d'entrée admise. Confirmer l'autorisation d'accès ou non. Appliquer tout autre identifiant inconnu du système au lecteur/clavier numérique/capteur biométrique et confirmer le refus de l'accès. La fonctionnalité doit être conforme au Tableau 4, lignes 14 à 17.

3) Vérifier que chaque tentative d'accès avec un jeton valide et des informations mémorisées non valides fait l'objet d'un refus. Vérifier qu'après le nombre de tentatives indiqué dans le Tableau 4 ligne 18, cet identifiant est bloqué conformément au(x) paramètre(s) défini(s) dans la configuration du système.

4) Examiner la documentation fournie par le fabricant et confirmer l'indication des niveaux FAR requis pour les dispositifs biométriques (lorsqu'ils sont utilisés avec l'unité de contrôle d'accès pour la classe appropriée). Les informations doivent être conformes au Tableau 4, ligne 20.

5) Examiner la documentation et vérifier que le nombre de différences de codes valides est satisfait pour le nombre d'utilisateurs admis par le système pour chaque classe. Les informations doivent être conformes au Tableau 4, ligne 21.

6) Examiner la documentation et vérifier que le nombre minimum de chiffres utilisés pour les informations mémorisées est conforme au Tableau 4, ligne 22.

7) Attribuer à 10 utilisateurs un jeton avec un code d'installation/utilisateur. Entrer un nouvel utilisateur/détenteur de carte et tenter d'attribuer au nouvel utilisateur un jeton déjà employé. Confirmer que le système refuse cette entrée et indique que ce jeton a déjà été attribué. La fonctionnalité doit être conforme au Tableau 4, ligne 24.

8) Attribuer des jetons avec des codes d'installation/utilisateur différents et le même code utilisateur à deux ou plusieurs utilisateurs. Confirmer que le système permet la saisie de codes d'installation différents. La fonctionnalité doit être conforme au Tableau 4, ligne 24.

9) Examiner la documentation fournie par le fabricant et confirmer la prise en charge ou non d'un mode de fonctionnement dégradé. Vérifier que le mode dégradé peut être désactivé automatiquement ou manuellement par un accès à niveau de surveillance, lorsque le système est examiné pour la fonctionnalité de classe 4. La fonctionnalité doit être conforme au Tableau 4, ligne 25.

10) Vérifier si la structure de codage des jetons destinés à être utilisés avec le système est visible (par exemple, jeton transparent), ou si le codage complet est imprimé sur le jeton. Les informations doivent être conformes au Tableau 4, lignes 26 et 27.

8.5.4 Critères de conformité

La fonctionnalité de reconnaissance doit être conforme aux exigences dépendant de la classification de sécurité indiquées en 6.4 et dans le Tableau 4.

8.6 Essais de fonctionnement pour le signalement d'agression

8.6.1 Objet de l'essai

Démontrer par inspection et essai qu'il est possible de satisfaire aux exigences concernant le signalement d'agression, indiquées en 6.5 et dans le Tableau 5.

8.6.2 Principes

La fonction d'agression du système de contrôle d'accès décrit à la Figure 3 doit être appliquée afin de démontrer que les sorties de ce système associées au signalement d'agression peuvent satisfaire aux exigences dépendant de la classification de sécurité indiquées dans le Tableau 5.

8.6.3 Mode opératoire (réf. Tableau 5, lignes 1 à 3)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 5, lignes 1 à 3, suivre les étapes suivantes:

1) Pour confirmer que le signalement d'agression est configurable, suivre les instructions du fabricant afin de programmer la fonction d'agression. La fonctionnalité doit être conforme au Tableau 5, ligne 1.

2) Fournir un élément d'agression en appliquant la méthode appropriée. Contrôler et consigner l'alerte reçue à la console de commande. Confirmer la distinction de l'alerte

d'agression par rapport aux autres alertes. La fonctionnalité doit être conforme au Tableau 5, ligne 2.

3) Confirmer, par essai et inspection, que le dispositif de déclenchement d'agression (par exemple, lecteur ou clavier numérique) ne produit pas d'indication locale sonore ou visible. La fonctionnalité doit être conforme au Tableau 5, ligne 3.

8.6.4 Critères de conformité

Le signalement d'agression doit être configurable accès contrôlé par accès contrôlé et les sorties d'alerte associées doivent être conformes aux exigences dépendant de la classification de sécurité indiquées dans le Tableau 5.

8.7 Essais de fonctionnement pour la neutralisation

8.7.1 Objet de l'essai

Démontrer par inspection et essai que le système de contrôle d'accès électronique peut satisfaire aux fonctionnalités de neutralisation de 6.6 et du Tableau 6.

8.7.2 Principes

Le système de contrôle d'accès décrit à la Figure 3 doit être utilisé pour démontrer que les fonctions de neutralisation dépendant de la classification de sécurité s'appliquent comme énumérées dans les exigences indiquées dans le Tableau 6.

8.7.3 Méthode d'essai (réf. Tableau 6, lignes 1 à 7)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 6, lignes 1 à 7, suivre les étapes suivantes:

1) Examiner la documentation fournie par le fabricant afin d'analyser le processus de neutralisation. Régler l'état d'un des lecteurs sur l'état de libre accès unique. Vérifier que la porte peut être soumise à une procédure d'accès et consigner alors cette vérification, puis réinitialiser cette procédure sur le processus d'autorisation d'accès normal. La fonctionnalité doit être conforme au Tableau 6, ligne 1.
2) Examiner la documentation fournie par le fabricant et déterminer l'indication selon laquelle l'installation et le fonctionnement du système EACS ne doivent pas empêcher la fonctionnalité des fonctions de sortie d'urgence. Les informations doivent être conformes au Tableau 6, ligne 5.
3) Examiner la documentation fournie par le fabricant afin de déterminer la prise en charge de la programmation des accès contrôlés dans le cas d'un accès bloqué temporisé. Saisir, pour l'un des points d'accès, l'heure et la date de début et de fin de blocage de l'accès.
4) Régler l'heure et la date 2 minutes avant le début de l'état de blocage de l'accès et vérifier l'autorisation effective de ce dernier. Vérifier, après le début de la période de blocage de l'accès, si celui-ci n'est pas autorisé pour plusieurs procédures d'accès.
5) Conformément au Tableau 6, ligne 7, régler l'heure et la date 2 minutes avant la fin de l'état de blocage de l'accès et vérifier la non autorisation de ce dernier. Vérifier, après la fin de la période de blocage de l'accès, si celui-ci est autorisé en cas d'application de la procédure d'autorisation d'accès normale.

8.7.4 Critères de conformité

La fonctionnalité de neutralisation doit être conforme aux exigences dépendant de la classification de sécurité indiquées en 6.6 et dans le Tableau 6.

8.8 Essais de fonctionnement pour la communication et l'autoprotection

8.8.1 Objet de l'essai

Démontrer par inspection et essai que le système de contrôle d'accès électronique peut satisfaire aux exigences concernant l'autoprotection de 6.7, 6.8 et du Tableau 7.

8.8.2 Principes

Le système de contrôle d'accès décrit à la Figure 3 doit être utilisé pour démontrer que les fonctions de communication et d'autoprotection dépendant de la classification de sécurité s'appliquent comme énumérées dans les exigences indiquées dans le Tableau 7.

8.8.3 Méthode d'essai (réf. Tableau 7, lignes 1 à 28)

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 7, lignes 1 à 28, suivre les étapes suivantes:

1) Lorsque le ou les composants de rétention de mémoire sont non volatils (exemple: EEPROM), vérifier les données fournies par le fabricant et vérifier également que les composants d'archivage sont non volatils pour la période requise par le Tableau 7, lignes 1 et 17.
2) Lorsque le ou les composants de rétention de mémoire sont volatils (exemple: RAM), enregistrer les paramètres de configuration du système et les événements archivés préalablement à la mise hors tension.
3) Déconnecter l'alimentation de secteur et les batteries de secours (les batteries de rétention des données doivent rester connectées) pendant la période requise par le Tableau 7, lignes 1 et 17.
4) Après la période définie par la classe de système appropriée, selon le Tableau 7, lignes 1 et 17, reconnecter l'alimentation de secteur et les batteries de secours. L'ordre de reconnexion doit être conforme aux recommandations du fabricant des équipements. La fonctionnalité doit être conforme au Tableau 7, ligne 2.
5) Comparer, par inspection, les paramètres de configuration du système et les événements archivés enregistrés, avec ceux du système de contrôle d'accès après remise sous tension. Les paramètres et le contenu du journal des événements ne doivent pas être perdus ou corrompus (à l'exception des événements de panne et de rétablissement d'alimentation) et l'horloge en temps réel doit continuer à afficher l'heure correcte.
6) Déterminer, en commun avec le fabricant du système de contrôle d'accès, une méthode permettant d'introduire ou de simuler des erreurs de somme de contrôle ou la perte de données. Par exemple, par la suppression des événements archivés de la mémoire non volatile, de sorte que le redémarrage correct de l'unité de contrôle d'accès n'est pas possible lors de la remise sous tension. La fonctionnalité doit être conforme au Tableau 7, ligne 3.
7) Examiner la documentation fournie par le fabricant pour référence à ou aux outils requis pour l'ouverture du boîtier de l'unité ou du composant de contrôle d'accès du système de même nature. La fonctionnalité doit être conforme au Tableau 7, ligne 4.
8) Installer le composant du système de contrôle d'accès selon les instructions du fabricant, avec le boîtier parfaitement fermé.
9) Ouvrir le boîtier par des moyens réguliers (en utilisant les outils et en suivant les instructions fournies par le fabricant) et tenter d'introduire un outil de sabotage (tige d'acier telle que définie dans la CEI 60529, d'un diamètre de 1 mm et d'une longueur de 100 mm) dans l'unité sans provoquer de dommage physique et avant que la détection d'inviolabilité ne fonctionne.
10) Lorsque l'outil est introduit avec succès, il convient de le manipuler de manière à tenter d'influer sur le mécanisme de détection d'inviolabilité ou d'autres composants internes, et de générer une condition d'autorisation d'accès. La fonctionnalité doit être conforme au Tableau 7, ligne 5.

11) Positionner l'unité ou le composant de contrôle d'accès du système de même nature sur une surface plane horizontale, compte tenu des exigences spécifiées par le fabricant afin de procéder au retrait du mécanisme de détection d'installation.

12) Soulever l'équipement de la surface plane perpendiculairement à la surface de montage et tenter de glisser un plat d'une largeur de 10 mm, d'une longueur de plus de 300 mm et d'une épaisseur de 1 mm, afin de neutraliser le retrait du mécanisme de détection d'installation. La fonctionnalité doit être conforme au Tableau 7, ligne 6.

13) Examiner la documentation fournie par le fabricant pour référence aux caractéristiques assignées IP et IK appropriées. Les informations doivent être conformes au Tableau 7, ligne 7.

14) Déconnecter la voie de communication entre l'unité de contrôle d'accès et le pupitre de contrôle. Générer, alors que la communication avec le pupitre de contrôle est interrompue, des demandes d'accès en utilisant des identifiants valides et vérifier que la fonctionnalité est conforme au point 3) de 6.7 et au Tableau 7, lignes 8, 20 et 21.

15) Rétablir la communication avec le pupitre de contrôle. La fonctionnalité doit être conforme au Tableau 7, ligne 8.

16) Examiner la documentation fournie par le fabricant afin de vérifier la capacité du nombre d'événements archivés dans l'unité de contrôle d'accès, la communication avec le pupitre de contrôle étant par ailleurs interrompue. La fonctionnalité doit être conforme au Tableau 7, ligne 8.

17) Le système de contrôle d'accès fonctionnant normalement selon la Figure 3, déconnecter le circuit de communication entre l'unité de contrôle d'accès et une interface (lecteur) de point d'accès pendant la durée indiquée dans le Tableau 7, ligne 9. Répéter l'essai s'il y a lieu pour les autres types de circuits de communication pris en charge par l'unité de contrôle d'accès. La fonctionnalité doit être conforme au point 4) de 6.7 et au Tableau 7, lignes 9, 18, 19 et 20.

18) Examiner la documentation fournie par le fabricant et confirmer la mise en œuvre des exigences selon le Tableau 7, lignes 24 et 25.

19) Examiner la documentation fournie par le fabricant et confirmer que les jetons acceptés par le système de contrôle d'accès et leur procédure d'initialisation satisfont aux exigences concernant la classe de sécurité selon le point 9) de 6.8 et le Tableau 7, ligne 19.

20) Examiner la documentation fournie par le fabricant et confirmer que l'accès à la configuration de l'unité de contrôle est limité par l'emploi d'identifiants valides (définis conformément à la classe de sécurité revendiquée), et qu'il est possible de limiter l'accès, par les niveaux d'accès, à différentes fonctions du système. La fonctionnalité doit être conforme au Tableau 7, lignes 10 à 16.

21) Vérifier que les règles de traitement mémorisées dans les lecteurs de points d'accès (par exemple, par l'intermédiaire de commutateurs DIP) ne sont pas visibles de l'extérieur du boîtier du lecteur lorsque celui-ci est en place. La conformité doit être telle que décrite dans le Tableau 7, ligne 22.

22) Confirmer par appui de chaque touche de clavier numérique que le son audible (lorsqu'il existe) est identique pour toutes les touches. La fonctionnalité doit être conforme au Tableau 7, ligne 23.

23) Tenter, avec le système de contrôle d'accès en mode configuration, de saisir des données non valides à partir de la console de commande (par exemple, autre qu'un format ou type de caractères pris en charge prévu), et confirmer la non acceptation des données par le système. La fonctionnalité doit être conforme au Tableau 7, ligne 27.

24) Accéder au mode configuration de la console de commande et ne saisir aucune donnée. Contrôler l'effet de la période d'inactivité sur le système. La fonctionnalité doit être conforme au Tableau 7, ligne 28.

8.8.4 Critères de conformité

Les fonctionnalités de communication et d'autoprotection doivent être conformes aux exigences dépendant de la classification de sécurité indiquées en 6.7, 6.8 et dans le Tableau 7.

8.9 Exigences concernant l'alimentation

8.9.1 Essai de la durée d'alimentation de secours

8.9.1.1 Objet de l'essai

Les exigences concernant l'alimentation de secours indiquées dans le Tableau 8, ligne 1, doivent être démontrées au moyen d'essais et par une inspection conformément au mode opératoire suivant.

8.9.1.2 Mode opératoire

Pour démontrer la capacité des alimentations utilisées avec le système de contrôle d'accès électronique à satisfaire aux exigences du Tableau 8, ligne 1, suivre les étapes suivantes:

1) Connecter au système de contrôle d'accès (sauf le pupitre de contrôle et les actionneurs de points d'accès) une source d'alimentation avec les batteries de secours du type et de la capacité recommandés par le fabricant. Les sorties des composants doivent être reliées aux charges représentatives des conditions maximales (I_{max}) relevant des spécifications du fabricant.
2) Le système de contrôle d'accès et ses accessoires doivent être contrôlés tout au long de l'essai afin d'identifier les changements d'état éventuels.
3) Charger les batteries reliées à l'alimentation de secteur nominale (V_n) pendant une durée minimale de 24 h.
4) Confirmer que le fonctionnement est correct en réalisant l'essai de fonctionnement réduit.
5) Déconnecter la source d'alimentation de secteur et confirmer l'absence de tout changement d'état involontaire.
6) Laisser le système de contrôle d'accès et ses accessoires fonctionner avec les batteries de secours pendant la durée définie par la classe de système appropriée définie dans le Tableau 8.
7) Confirmer, immédiatement après le fonctionnement sur les batteries de secours pendant la durée requise, le fonctionnement correct de l'unité de contrôle d'accès et de ses accessoires en réalisant l'essai de fonctionnement réduit.
8) Reconnecter la source d'alimentation de secteur et confirmer à nouveau l'absence de tout changement d'état involontaire.

8.9.1.3 Critères de conformité

Les exigences de l'essai de fonctionnement réduit doivent être satisfaites suite à la période de fonctionnement avec les batteries de secours et aucun changement d'état involontaire ne doit s'être produit.

8.9.2 Essai de capacité du chargeur et de la source d'alimentation de secours

8.9.2.1 Objet de l'essai

Les exigences concernant la capacité de recharge indiquées dans le Tableau 8, ligne 2, doivent être démontrées au moyen d'essais et par une inspection conformément au mode opératoire suivant.

8.9.2.2 Mode opératoire

Pour démontrer la capacité de l'unité de contrôle d'accès à satisfaire aux exigences du Tableau 8, ligne 2, suivre les étapes suivantes:

1) Une batterie de la capacité maximale recommandée par le fabricant des équipements doit être utilisée.
2) Décharger la batterie à sa tension finale à un courant de décharge de I_d = C/20 A pour les batteries au plomb, (ou I_d = C/10 A pour les batteries au nickel-cadmium), où C est la capacité en ampère-heure assignée de la batterie, donnée par le fabricant de batteries.
3) Pour les autres types de batterie, le courant de décharge doit être celui pour lequel le fabricant de batteries spécifie la capacité assignée.
4) Charger la batterie pendant 72 heures, le chargeur approprié étant relié au secteur nominal (V_n) tandis que la sortie d'alimentation est chargée par I_{max}.
5) Répéter le mode opératoire comme décrit à l'étape 2) ci-dessus et mesurer le temps de décharge (T_1) en heures.
6) Charger à nouveau la batterie pendant 24 heures à V_n tandis que les sorties du système de contrôle d'accès sont chargées par $I_{max.}$.
7) Décharger à nouveau la batterie à sa tension finale à un courant de décharge comme décrit à l'étape 2) ci-dessus et mesurer le temps de décharge (T_2) en heures

8.9.2.3 Critères de conformité

Le produit du temps de décharge T_1 et du courant de décharge I_d ne doit pas être inférieur à:

a) 100 % de la capacité assignée de la batterie après chargement pendant une durée de 72 heures, et
b) 80 % de la capacité assignée de la batterie après chargement pendant une durée de 24 heures.

8.9.3 Essai de batterie faible ou manquante

8.9.3.1 Objet de l'essai

Démontrer que des moyens de contrôle et de signalement de la présence d'une batterie faible sont prévus, comme requis par le Tableau 8, ligne 3.

8.9.3.2 Mode opératoire

Le mode opératoire suivant doit être appliqué aux systèmes de contrôle d'accès intégrant des batteries de secours:

1) Le cas échéant, remplacer les batteries de secours par une alimentation variable réglée à la tension d'alimentation nominale recommandée (V_{nom}).

   NOTE Certains types de source d'alimentation par batterie ne peuvent pas être simulés par le remplacement d'une alimentation variable, par exemple, batteries au lithium. Des méthodes différentes de démonstration de la conformité sont, si nécessaire, admises sous réserve de l'accord entre le demandeur et le laboratoire d'essai.

2) Confirmer le fonctionnement correct du système de contrôle d'accès par réalisation de l'essai de fonctionnement réduit.
3) Réduire lentement le niveau de V_{nom} à un débit de 10 mV/s environ jusqu'à l'indication de la présence d'une batterie faible sur un écran local et/ou à la console de commande.
4) Enregistrer la tension d'indication de la présence d'une batterie faible (V_{low}) et appliquer l'essai de fonctionnement réduit.
5) Retirer entièrement les batteries de secours du système de contrôle d'accès et répéter l'étape 4).

8.9.3.3 Critères de conformité

Le système de contrôle d'accès doit avoir signalé toute indication de dysfonctionnement de batterie, toute alerte et tout événement enregistré dans le journal, en réponse à la présence d'une batterie faible avant que tout fonctionnement correct soit empêché. Le système de contrôle d'accès doit continuer à satisfaire aux exigences de l'essai de fonctionnement réduit avec la tension de service réglée sur V_{low}. La détection d'une batterie manquante doit engendrer une indication de dysfonctionnement de batterie, une alerte et un événement enregistré dans le journal.

8.10 Exigences concernant l'environnement et la CEM (immunité)

8.10.1 Mode opératoire

Les essais concernant l'environnement et la CEM spécifiés dans le Tableau 9 doivent être réalisées comme suit:

1) L'appareil d'essai et les modes opératoires doivent être tels que décrits dans la CEI 62599-1 et la CEI 62599-2. Appliquer les essais indiqués dans le Tableau 9.
2) Sauf indication contraire du mode opératoire, les essais doivent être effectués à la tension d'alimentation assignée pour le composant.
3) Les niveaux de sévérité à appliquer sont définis par quatre niveaux de la classe d'environnement I à la classe d'environnement IV:
   a) classe I: intérieur, mais limité à un environnement de type résidentiel/de bureau (par exemple, salons et bureaux);
   b) classe II: intérieur en général (par exemple, lieux de vente, boutiques, restaurants, escaliers, lieux de fabrication et d'assemblage, entrées et aires de stockage);
   c) classe III: extérieur, mais abrité de l'exposition directe à la pluie et au soleil, ou à l'intérieur mais avec des conditions extrêmes d'environnement (par exemple, garages, greniers, granges et quais de chargement);
   d) classe IV: à l'extérieur en général.
4) Les interconnexions de systèmes à des fins d'essai (c'est-à-dire à des entrées et sorties) doivent être réalisées au moyen de câbles non blindés, à moins que les données d'installation du fabricant ne spécifient que seuls des câbles blindés doivent être utilisés.
5) Lorsque les équipements comportent un certain nombre de types d'entrées ou de sorties identiques, les essais doivent être réalisés sur au moins une entrée et une sortie représentative de chaque type.

8.10.2 Mesures initiales

Outre les critères de conformité spécifiés dans la CEI 62599-1 et la CEI 62599-2, l'essai de fonctionnement décrit au 8.2 doit être réalisé pendant les mesures initiales.

8.10.3 Etat de l'éprouvette en cours de conditionnement

Monter la ou les éprouvettes conformément aux instructions du fabricant et les connecter à une source d'alimentation adaptée telle que recommandée dans la documentation fournie avec le système de contrôle d'accès électronique.

8.10.4 Conditionnement

Les mesures suivantes doivent être observées lors de la réalisation des essais exigés dans le Tableau 9:

1) Les éprouvettes pour essai doivent être exposées au conditionnement et aux essais spécifiés dans le Tableau 9 en utilisant les méthodes décrites dans la CEI 62599-1 et la CEI 62599-2.

2) Le conditionnement d'impact fonctionnel doit être appliqué à tous les composants du système de contrôle d'accès. Toutefois, les impacts ne doivent pas être appliqués directement sur les écrans (par exemple, écrans à cristaux liquides) ou d'autres types d'indicateurs visuels.

3) Les décharges électrostatiques doivent être appliquées aux seules parties des équipements de contrôle d'accès susceptibles d'être accessibles à l'utilisateur final lorsqu'elles sont installées en tant que système.

4) Les rafales transitoires rapides doivent être appliquées aux lignes de réseau en courant alternatif par la méthode à injection directe et aux autres entrées, lignes de signal, de données et de commande par la méthode à serrage capacitif.

8.10.5 Mesure en cours de conditionnement

Contrôler l'éprouvette pendant la période de conditionnement afin de détecter toute autorisation d'accès, toutes alertes ou tous signaux de panne.

8.10.6 Mesures finales

Outre les critères de conformité spécifiés dans la CEI 62599-1 et la CEI 62599-2, l'essai de fonctionnement décrit au 8.2 doit être réalisé pendant les mesures initiales et finales.

8.10.7 Critères de conformité

8.10.7.1 Essais de fonctionnement

Le système de contrôle d'accès ne doit pas, de manière involontaire, autoriser un accès, générer une alerte, des signaux anti-violation, de panne ou d'autres signaux ou messages, ou passer d'un mode à un autre, et doit continuer à fonctionner normalement lorsqu'il est soumis à la plage spécifiée de conditions d'environnement et de conditions CEM.

8.10.7.2 Essais d'endurance

Le système de contrôle d'accès doit satisfaire à l'essai de fonctionnement réduit après avoir été soumis à la plage spécifiée de conditions d'environnement.

8.11 Rapport d’essai

Il doit contenir au minimum les informations suivantes:

a) l'identification de l'éprouvette pour essai, l'état de constitution et les versions de micrologiciel/logiciel;

b) référence à la présente partie de la CEI 60839;

c) la classification du ou des composants évalués du système de contrôle d'accès;

d) les résultats d'évaluation des exigences de la présente partie de la CEI 60839;

e) les résultats des essais, et les autres données éventuelles, comme spécifié dans les essais individuels;

f) les période et atmosphère de conditionnement;

g) les détails des équipements d'alimentation et de contrôle, et les critères de réponse;

h) les détails de tout écart par rapport à la présente partie de la CEI 60839 ou aux normes internationales auxquelles il est fait référence, et les détails des opérations considérées comme facultatives.

9 Documentation et marquage

9.1 Documentation

Le fabricant doit élaborer la documentation d'installation et d'utilisation, qui doit accompagner l'unité de contrôle d'accès. Cette documentation doit comporter au moins les informations suivantes:

a) la description générale des équipements, y compris une liste des
   - fonctions obligatoires pour la classe à laquelle les équipements satisfont;
   - fonctions facultatives de la présente partie de la CEI 60839;

b) les spécifications techniques des entrées et sorties de l'unité de contrôle d'accès, suffisantes pour permettre une évaluation de la compatibilité mécanique, électrique et logicielle avec les autres composants du système, y compris le cas échéant:
   - les exigences concernant l'alimentation pour le fonctionnement recommandé;
   - le nombre maximum de points d'accès, dispositifs de libération;
   - les caractéristiques électriques assignées maximales et minimales pour chaque entrée et chaque sortie;
   - les informations concernant les paramètres de communication utilisés sur chaque trajet de transmission;
   - les paramètres de câble recommandés pour chaque trajet de transmission;
   - les caractéristiques assignées de fusibles;

c) les informations concernant l'installation, y compris
   - la température de service et la plage d'humidité;
   - la classe d'environnement;
   - les caractéristiques assignées IP/IK auxquelles les équipements satisfont;
   - les instructions de montage;
   - les instructions concernant la connexion des entrées et sorties;

d) les instructions de configuration et de mise en service;

e) les instructions de fonctionnement;

f) les informations de service.

Le fabricant doit élaborer la documentation de conception qui doit être soumise au laboratoire d'essai, avec l'équipement de contrôle d'accès. Cette documentation doit inclure les dessins, nomenclatures, schémas fonctionnels, schémas de circuit, ainsi qu'une description fonctionnelle permettant de vérifier la conformité avec la présente partie de la CEI 60839, et de procéder à une évaluation générale de la conception électrique et mécanique.

9.2 Marquage

Le composant d'un système de contrôle d'accès doit comporter un marquage comprenant les informations suivantes:

a) la norme à laquelle le composant revendique la conformité (c'est-à-dire CEI 60839-11-1);

b) le type de composant (par exemple, unité de contrôle d'accès, lecteur de cartes, etc.);

c) le nom ou la marque du fabricant ou du fournisseur;

d) la classe;

e) la classe d'environnement;

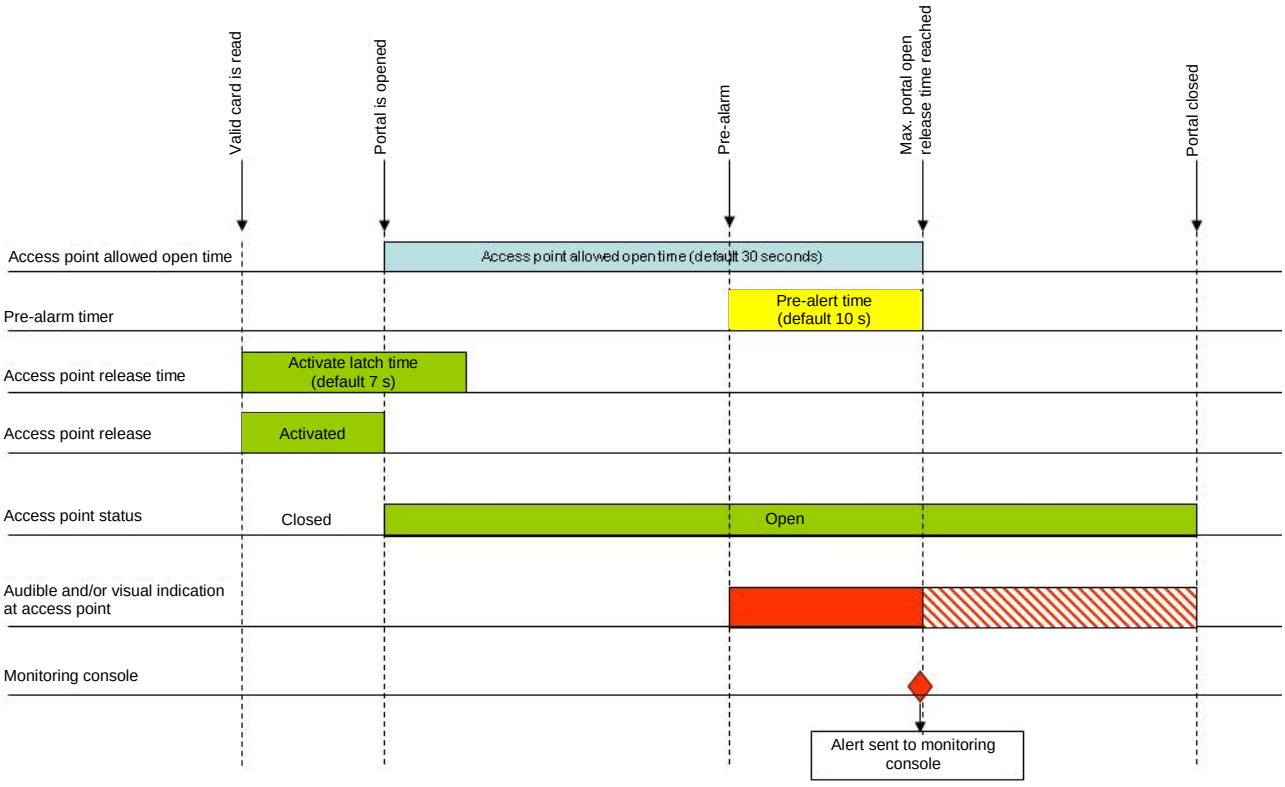
f) la date de fabrication, le numéro de lot ou le numéro de série.

Le marquage doit être lisible, durable et non ambigu. Lorsque l'espace de marquage du composant d'un système de contrôle d'accès est restreint, des codes peuvent être employés

sous réserve qu'ils soient décrits dans la documentation du composant associée. Lorsque l'espace pour les codes est insuffisant, le composant doit comporter des moyens d'identification qui permettent une référence croisée à la documentation qui fournit les informations requises.

Annexe A
(normative)

Chronogramme



IEC 926/13

NOTE Le temps de pré-alerte peut être considéré comme faisant partie intégrante du temps d'ouverture admise de l'accès contrôlé, ou comme suivant cette période. Ceci peut altérer les paramètres de temps qui doivent être conformes aux exigences du Tableau 2.

L'indication de pré-alerte locale sonore et/ou visible peut s'interrompre au moment de la transmission de l'alerte à la console de commande ou de la fermeture de l'accès contrôlé.

Légende

Anglais	Français
Valid card is read	Lecture de carte valide
Portal is opened	Ouverture de l'accès contrôlé
Pre-alarm	Pré-alarme
Max. portal open release time reached	Temps de libération maximal de l'accès contrôlé ouvert atteint
Portal closed	Accès contrôlé fermé
Access point allowed open time	Temps d'ouverture admise du point d'accès
(default 30 s)	(30 s par défaut)
Pre-alarm timer	Temporisateur de pré-alarme
Pre-alert time	Temps de pré-alerte

Anglais	Français
(default 10 s)	(10 s par défaut)
Access point release time	Temps de libération du point d'accès
Activate latch time (default 7 s)	Activer temps de verrouillage (7 s par défaut)
Access point release	Libération du point d'accès
Activated	Activé
Access point status	Etat du point d'accès
Closed	Fermé
Open	Ouvert
Audible and/or visual indication at access point	Indication sonore et/ou visuelle au point d'accès
Monitoring console	Pupitre de contrôle
Alert sent to monitoring console	Alerte transmise à la console de commande

Figure A.1 – Chronogramme

Bibliographie

CEI 60839-11-2, *Systèmes d'alarme et systèmes de sécurité électroniques – Partie 11-2: Systèmes de contrôle d'accès électronique – Lignes directrices d'application*

CEI 60950-1, *Matériels de traitement de l'information – Sécurité – Partie 1: Exigences générales*

CEI 61000-6-1, *Compatibilité électromagnétique (CEM) – Partie 6-1: Normes génériques – Immunité pour les environnements résidentiels, commerciaux et de l'industrie légère*

CEI 61000-6-3, *Compatibilité électromagnétique (CEM) – Partie 6-3: Normes génériques – Norme sur l'émission pour les environnements résidentiels, commerciaux et de l'industrie légère*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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