IEC 60839-11-2

Edition 1.0 2014-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC 60839-11-2:2014-07(en-fr)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online 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 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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 l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC 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.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. 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 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 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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 60839-11-2

Edition 1.0 2014-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

U

ICS 13.320

ISBN 978-2-8322-1774-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-2: Electronic access control systems – Application guidelines

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 60839-11-2 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
79/476/FDIS	79/489/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 planning, installation, operation, maintenance and documentation for the application of electronic access control systems (EACS).

The performance of the EACS is determined by the security grades allocated to the access points. A risk assessment that identifies the risks and perceived threats should first be carried out in order to establish the appropriate security grades.

Four security grades are available based upon the knowledge and tools available to a person intent upon gaining unauthorised access and the type of application, taking into account specific organizational aspects and the value of the assets.

Separate guidance is provided for each activity along with recommendations for the documentation needed. A brief description of each section covering the activities is provided below:

System planning: this section is intended to assist the designer with the selection of an electronic access control system (EACS) that provides the control of access and security integrity commensurate with the value of the assets requiring protection and the associated risks. See Clause 7.

System design should minimise potential vulnerabilities that could be exploited to circumvent the access control measures. It is recommended that safeguards are incorporated to give early warning of attempts to circumvent the access control measures. See 7.3.

System installation: this section is intended to help those responsible for installing the EACS by identifying issues which should be considered prior to commencing the installation and during the installation of the system in order to ensure the EACS is correctly implemented as specified during system planning. See Clause 8.

Commissioning and system handover: this section provides guidance to ensure the level of performance required in the system planning is obtained and that the end user is provided with the necessary documentation, records and operating instructions during the handover of the EACS. See Clause 9.

System operation and maintenance: includes information regarding the responsibilities of the end user of the EACS to ensure the system is operated correctly and adequately maintained. It covers inspection, service and the use of remote diagnostics in order that the level of performance determined during the system planning stages can be maintained. See Clause 10.

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-2: Electronic access control systems – Application guidelines

1 Scope

This part of IEC 60839 defines the minimum requirements and guidance for the installation and operation of electronic access control systems (EACS) and/or accessory equipment to meet different levels of protection.

This standard includes requirements for planning, installation, commissioning, maintenance and documentation for the application of EACS installed in and around buildings and areas. The equipment functions are defined in the IEC 60839-11-1.

When the EACS includes functions relating to hold-up or the detection of intruders, the requirements in standards relating to intrusion and hold-up are also applicable.

This standard provides application guidelines intended to assist those responsible for establishing an EACS to ascertain the appropriate design and planning of the EACS, both in terms of levels of protection and levels of performance necessary to provide the degree of access control and protection considered appropriate for each installation. This is achieved by scaling or classifying the features of electronic access control systems related to the security functionality (e.g. recognition, access point actuation, access point monitoring, duress signaling and system self-protection) in line with the known or perceived threat conditions.

This standard does not cover the methods and procedures for conducting a risk assessment.

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 60839-11-1:2013, *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*

3 Terms and definitions

For the purposes of this document the terms and definitions given in IEC 60839-11-1, as well as the following, apply.

3.1
area zone
part of a protected area which has its own set of access levels

Note 1 to entry: It may have a different security grade than other area zones within the same protected area.

3.2
competent organization
organization possessing sufficient resources and staff with adequate expertise and training in the maintenance of EACS

3.3
fail-safe
fail-open
locking device designed to automatically release upon power failure

3.4
fail-secure
fail-locked
locking device designed to remain secure upon power failure

3.5
protected area
controlled area
area defined by a physical boundary, through which passage is controlled by means of one or more access points/portals

Note 1 to entry: It may contain several separate area zones with the same or different security grades. Refer to the area zone definition in 3.1.

3.6
system owner
person or group of people that make the decision about what is appropriate for the respective premises to be used in order to get the desired access control/protection/price/etc.

4 Abbreviations

For the purposes of this document, the abbreviations given in IEC 60839-11-1, as well as the following apply.

ACU Access control unit

EACS Electronic access control system

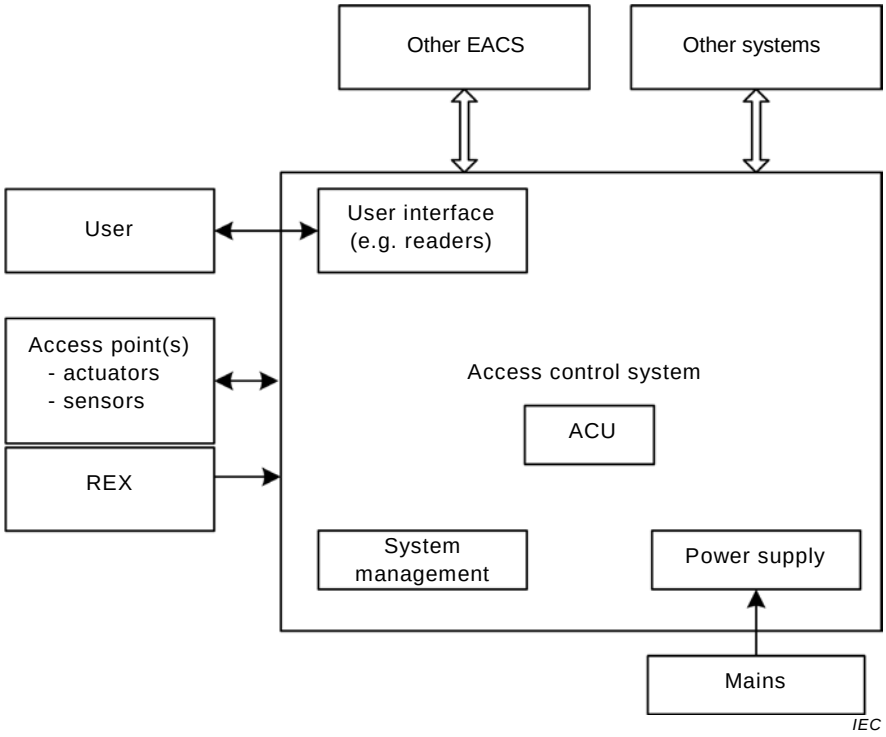
EMC Electromagnetic compatibility

REX Request to exit

5 System architecture

An access control system comprises all the constructional and organizational facilities together with equipment required for controlling access. Refer to Figure 1 for an example of a typical arrangement of components and interfaces of an EACS.

The physical protection and mechanical strength of actuators, sensors, etc., should be commensurate for the security grade of each access point. Consideration should be given to the physical strength of the surrounding building (e.g. walls, door construction, etc).



IEC 60839-11-1:2013, Table 8, states that: "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" required according to the security grade of the EACS. It is recommended that monitored standby power sources be provided to all actuators and monitoring console(s).

Figure 1 – Typical arrangement of components and interfaces of an EACS

6 Environmental and EMC considerations

6.1 General

Each component of an EACS is expected to operate correctly in its service environment and that it will continue to do so for a reasonable time. Components shall be suitable for one of the following environmental classes.

6.2 Environmental Class I – Equipment situated in indoor but restricted to residential/office environment

Environmental Class I comprises environmental influences normally experienced indoors when the temperature is well maintained (e.g. in a residential or commercial property).

NOTE Temperatures can be expected to vary between +5 °C and +40 °C.

6.3 Environmental Class II – Equipment situated indoor in general

Environmental Class II comprises environmental influences normally experienced indoors when the temperature is not well maintained (e.g. in corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent).

NOTE Temperatures can be expected to vary between –10 °C and +55 °C.

6.4 Environmental Class III – Equipment situated outdoor – Sheltered or indoor extreme conditions

Environmental Class III comprises environmental influences normally experienced out of doors when the EACS components are not fully exposed to the weather or indoors where environmental conditions are extreme.

NOTE Temperatures can be expected to vary between –25 °C and +55 °C.

6.5 Environmental Class IV – Equipment situated outdoor – General

Environmental Class IV comprises environmental influences normally experienced out of doors when the EACS components are fully exposed to the weather.

NOTE Temperatures can be expected to vary between –25 °C and +70 °C depending on the region. The temperature range can be extended to plus and/or minus for different geographical or climatic zones.

6.6 EMC

It is recommended that installation good practice be followed to reduce the unwanted effects of electrical interference, e.g. interconnection wiring should not be run in the same conduit or trunking as cables carrying mains supplies, or network and data cables carrying high frequency signals unless they are physically separated and/or suitably screened so as to prevent cross interference.

Additional filtering and/or screening of interconnecting cables might be necessary for applications known to have high levels of conducted or radiated electrical interference, e.g. an industrial plant operating high power electrical equipment.

The manufacturers' guidelines for electromagnetic compatibility should be followed.

7 System planning

7.1 General

The objectives of the system planning stage are to determine the extent of EACS, to select components of the appropriate functionality/performance criteria, security grade and environmental classification and to prepare a system design proposal.

An access control system comprises all the logical functionality, constructional and organizational facilities together with the physical equipment required for controlling access.

Particular care should be taken to minimize inconvenience to authorized users.

The implementation of an access control system should be in accordance with the following sequence:

a) risk assessment and security grading;
b) system and components selection;
c) operational considerations;
d) system installation;
e) system handover;
f) system operation and maintenance.

System installation shall be conducted in accordance with national and local regulations.

7.2 Risk assessment and security grading

It is essential that a risk assessment is performed before the implementation of the access control system. The risk assessment chart of Figure 2 identifies the key considerations.

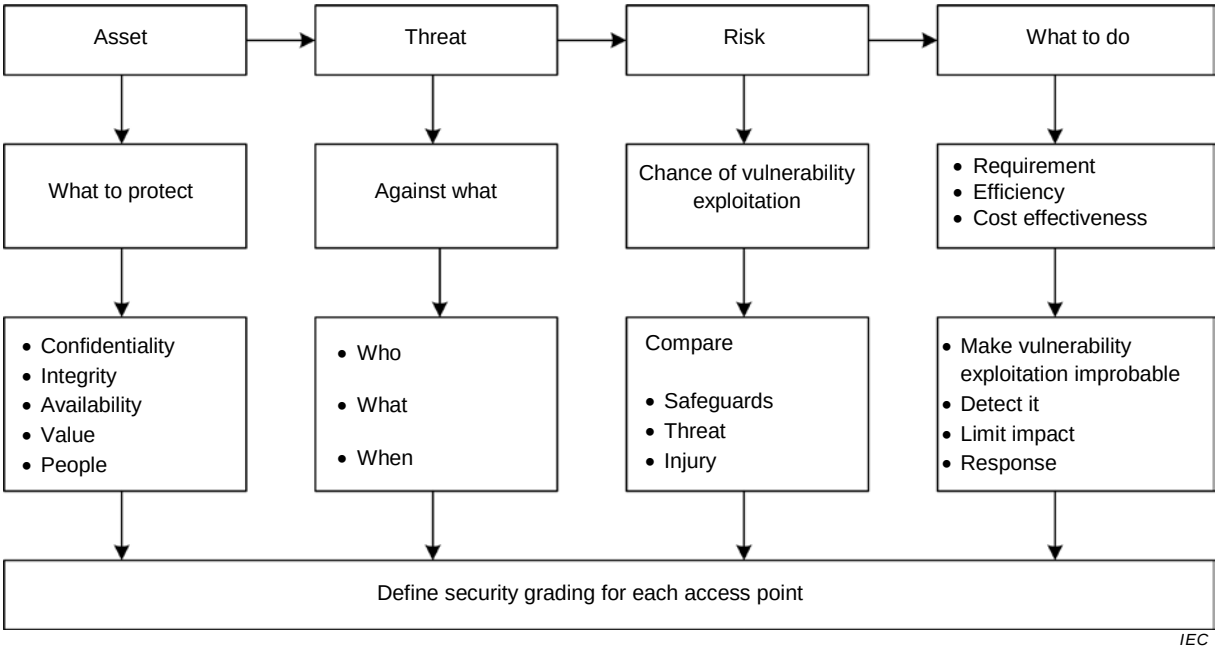


Figure 2 – Risk assessment chart

The security grade 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). Refer to Table 1 for examples of typical applications for each grade.

– 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. Physical security is provided to deter and delay adversaries. Assets have limited value and adversaries 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. Physical security is provided to deter, delay and detect adversaries. The assets have higher value and adversaries are likely to 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 the access control system and have a comprehensive range of tools and portable electronic equipment. Physical security is provided to deter, delay, detect and means are provided to help identify adversaries. The assets have high value and adversaries 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. Physical security is provided to deter, delay, detect and means are provided to help identify adversaries. The assets have very high value and adversaries may give up the idea of succeeding when they realize they will be identified and caught.

Table 1 – Security grading

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 EACS, no knowledge of token and IT technologies. Low financial means for attacks	Medium skill and knowledge of EACS, low knowledge of token and IT technologies. Low to medium financial means for attacks	High skill and knowledge of EACS, medium knowledge of token and IT technologies. Medium financial means for attacks	Very high skill and knowledge of EACS, 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)

7.3 System design

7.3.1 System and components selection

The security grading shall be defined for each access point taking in consideration the needs for control of entry and exit.

Different security grades can be used for access points in the same system. It shall be ensured that the common system components, protecting access points with different security grading, meet the requirements of the highest security grade access point that they are operating in conjunction with (see Figure 3).

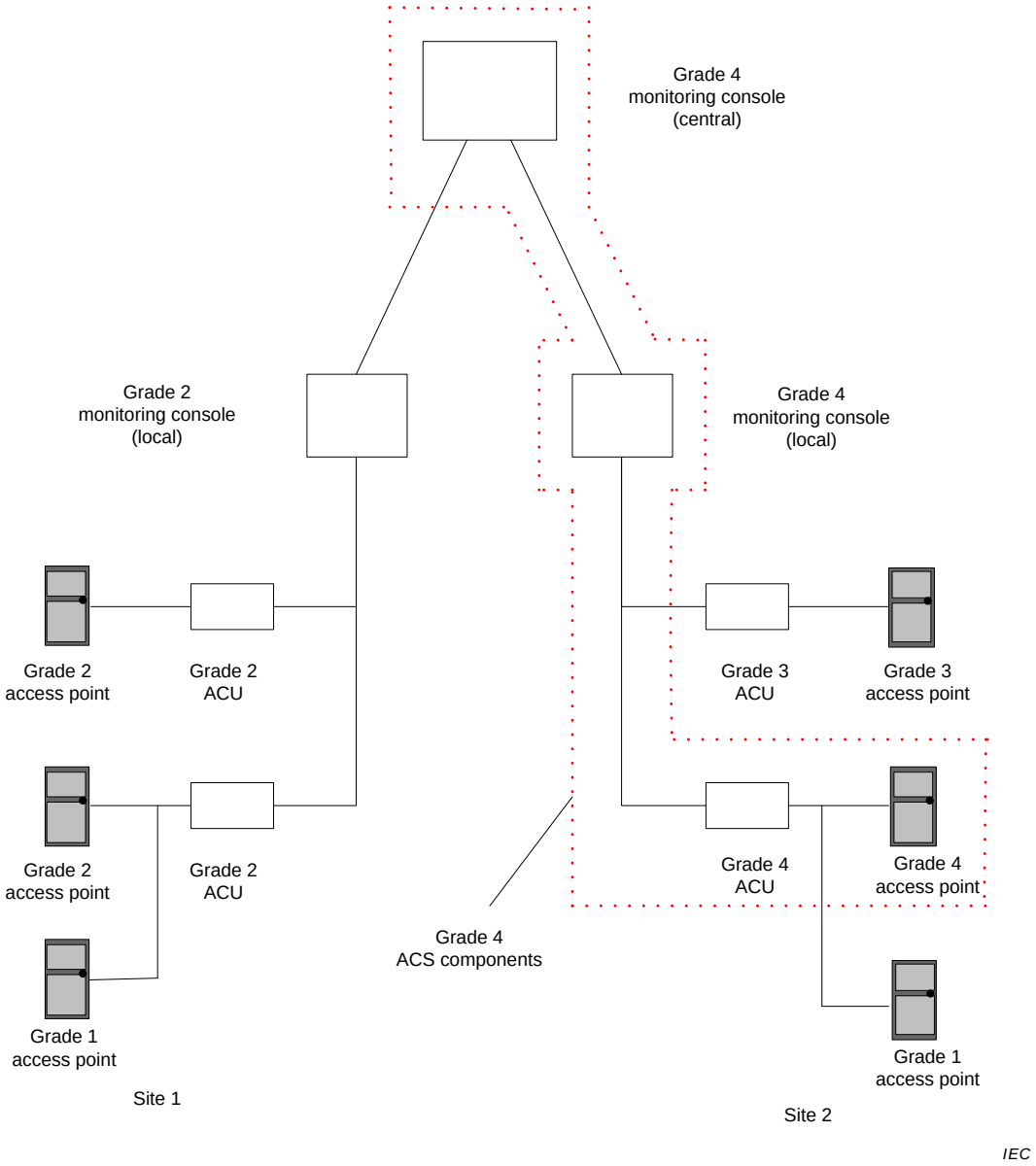


Figure 3 – Example of system grade selection

Where it is not practical to have different grades of access points managed by a single access control system it is permitted to have more than one separate access control system. An access point shall not be controlled by more than one separate access control system.

The mandatory functions of the equipment associated with each security grade are defined in the IEC 60839-11-1.

Not all mandatory functions defined in the IEC 60839-11-1 need to be implemented in an installed EACS. A list of allowed exceptions is provided in Annex A. Exceptions shall be agreed between the installer and the system owner and be recorded in the as-built documentation.

The installer shall point out to the system owner that exceptions from the requirements, especially for access points, recognition and communication, may affect the functions and the security of the whole EACS.

7.3.2 Operational considerations

7.3.2.1 General

The operational considerations in this subclause are guidelines for points of discussion with the customer in order to understand and address the needs of the final installation.

These guidelines have also to be reviewed in conjunction with the mandatory functions for each security grade of the EACS as specified in the IEC 60839-11-1.

The guidelines are not exhaustive and are not listed in any order of priority.

7.3.2.2 Guidelines

The following items should be considered:

a) manufacturer's recommendations;
b) the threat(s);
c) specific assets requiring protection;
d) activities undertaken at the site/building;
e) access control measure philosophy;
f) security grade for each access point;
g) user flow (number of persons in a period of time);
h) operation of the access control system while under fault conditions (e.g. the need for a second source of power, equipment cable infrastructure, loss of communication, etc.);
i) access control for users with disabilities;
j) safety requirements (e.g. emergency exits, fire protection, etc.);
k) environmental and EMC conditions of the site;
l) redundancy, disaster recovery plans for monitoring console;
m) location of the equipment (control unit, user interface, monitoring console);
n) co-operation of users (motivation, training, etc.);
o) training of operators;
p) the cable routes, the type of cable, the maximum cable length;
q) the communication links (availability, reliability, security, performance);
r) tamper detection;
s) alarm/alert reporting method;
t) throughput of personnel (staff and visitors);
u) management of visitors;
v) response force (e.g. police) arrangements;
w) vehicle access;
x) access levels (authorization) for each area zone.

7.3.2.3 Regulatory requirements

Attention should be paid to any applicable international, national and local regulatory requirements including:

a) measures for persons with disabilities;
b) data protection and privacy legislation;
c) industry specific regulations;

d) health and safety, safe exit in emergency conditions.

7.3.2.4 Recognition

When selecting the recognition equipment and methods the following should be considered:

a) the suitability of the recognition equipment for the specific application including convenience of use, anticipated user flow, the operating environment and expected life time of the equipment, etc;

b) the methods of recognition, for example the use of pin only, token/card only, biometrics or a combination of methods (i.e. multi-factor).

7.3.2.5 System management

To maintain the continued and reliable operation of the EACS adequate system management is required and the following items should be considered when applicable:

a) operation of and responsibility for the system (programming, credentials management, access rights administration, configuration, alarm management day and night);

b) skills and training of system operators;

c) reporting;

d) archiving and back-up policy;

e) the number of users and access levels taking into account both present and predicted future needs;

f) ease of operation (user, management, serviceability, etc.);

g) requirements for annunciation (e.g. display, logging, alert, etc.);

h) the capacity of the logging device;

i) co-ordination of annunciation functions (location, procedures, presentation, etc.);

j) override.

7.3.2.6 Access point(s)

For proper installation and operation of the access points the following items should be considered:

a) requirements for indication;

b) operation during fault conditions;

c) other relevant factors (e.g. risk of vandalism, etc.);

d) physical strength;

e) surrounding building structure;

f) selection of appropriate access point actuators, i.e. locks, door strikes (security level, appearance, operating environment, operating response times, requirements to fit on existing structure);

g) safety requirements (e.g. emergency exits, fire protection, etc.);

h) access point monitoring;

i) detection/prevention of two or more persons attempting simultaneous entry (i.e. singularisation);

j) method of returning the access point to the closed condition (e.g. automatic door closing equipment);

k) operating configuration in the event of power failure (fail-safe, fail-secure....);

l) measures for persons with disabilities;

m) specific measures for handling deliveries;

n) the security classification for access points leading to the same security controlled area;

o) additional recognition/detection measures (weight, metal detection, image comparison, visual inspection, etc.);

p) anti-passback (logical, timed, area controlled);

q) override;

r) duress alarm;

s) two users access condition;

t) presence check.

7.3.2.7 Interface with other systems

When it is necessary to interface the EACS with other systems such as intrusion alarm systems, video surveillance systems, administration systems, intercom, elevator control, etc. consideration should be given to the following:

a) the type of communication links, the desired availability, reliability and security of transmitted data associated with those links;

b) the network infrastructure requirements;

c) specific operating commands for example, call for elevator, selection of floor and destination;

d) reporting commands associated with elevator control.

8 System installation

8.1 General

Prior to commencing work, all relevant safety requirements should be considered.

Electrical installation methods shall comply with current national and site local regulations.

The components of the EACS should be installed in locations that ensure adequate security of operation and permit easy access for maintenance and service.

All system components should be suitable for the environmental conditions in which they are to operate.

Care should be taken during the selection of components to ensure all system components are compatible. Where uncertainty arises the appropriate consultation should take place, e.g. with the component manufacturer, supplier, a test house or another relevant third party.

The results of the risk assessment shall determine the security grades of the area zones within the protected area. The access points to those area zones shall be of an equivalent grade or higher. For each area zone separate access levels may be defined.

With the exception of the user interface, equipment critical to the security integrity of the access control system shall not be located within an area zone designated as having a lower security grade than the highest grade of the protected area it is controlling. Refer to Figure 4.

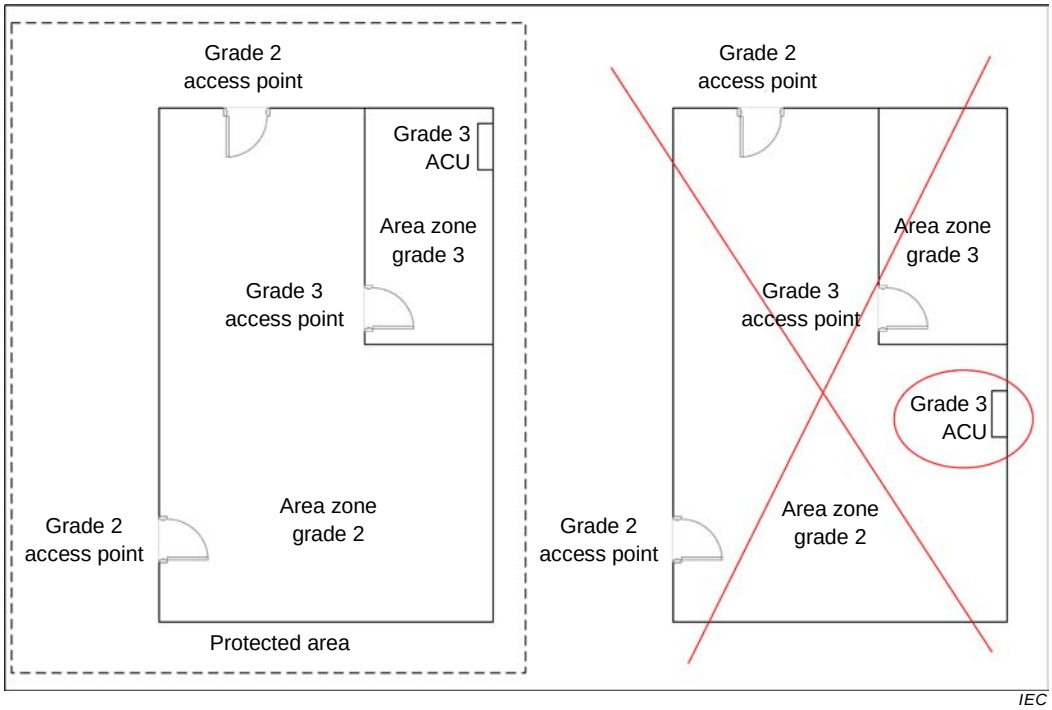


Figure 4 – Equipment location versus security grade of protected area

The installer shall make the system owner aware of any specific functionality that shall be implemented in order to meet the necessary organizational and constructional measures that are required for the proper operation of the EACS. For example the detection/prevention of two or more persons attempting simultaneous entry (singularisation) is recommended for the implementation of anti-tailgating measures.

Consideration should be given to routing cables only within the protected area (see 8.2.2).

8.2 Installation planning

8.2.1 Equipment

The equipment used in installations covered by this standard shall be compliant with the requirements covered by IEC 60839-11-1 for the applicable security grade and environmental classification.

The equipment should be installed in accordance with the manufacturer's instructions by suitably trained personnel. If the installation of a component in accordance with the manufacturer’s recommendations is not possible advice should be sought from the manufacturer and this should be recorded in the as-built documentation.

When the EACS is using existing communication (network) infrastructure at the customer site attention should be paid to ensure there are sufficient capacity, performance and protection measures in place to allow proper operation of the EACS for the selected security grade.

The housings for components of an EACS shall be provided with the means to prevent undetected access to internal elements to minimise the risk of tampering. The requirements for tamper protection may vary dependent on the security grade of the EACS and whether a component of the system is located within or outside of the security controlled area.

Provision should be made when planning the access control system to allow controlled access to protected areas in the event of a system malfunction or failure.

Power supplies should be located within the security controlled area. Where this is impractical, additional measures should be taken to maintain a security level equivalent to the security controlled area.

The ratings of the power supplies should be selected to meet the electrical specification of each associated component at the largest load expected under normal operating conditions.

NOTE Normal operating condition is when all the EACS equipment is fully functional and being used as intended with the maximum number of people entering and exiting via the controlled access points and as specified in the design documentation.

Power supplies with mains connections should use a dedicated, separately protected electrical circuit.

Consideration shall be given to the standby power requirements of the installed EACS and its associated communication network components.

Standby power supplies shall be capable of supporting the access control unit(s) and accessories, including actuators operating under specified operating load conditions for the period of time required applicable to the security grade of the installed EACS as stated in Table 2.

Table 2 – Power supply requirements for installed EACS

Standby power supply requirements	Grade assignment			
	1	2	3	4
EACS required to continue operating in the event of a failure of the primary source	OP	OP	M [a]	M [a]
Standby power sources shall be capable of operating under specified load conditions for the period of time indicated	OP	OP	2 h [b]	4 h

[a] Some types of actuators may be excluded from the grade dependent standby power requirements (e.g. AC powered and/or high power consuming) provided it has been agreed between the system owner and the installer and recorded in the 'as-built' documentation.

[b] A shorter standby time may be acceptable provided it has been agreed between the system owner and the installer and also recorded in the 'as-built' documentation.

The EACS may have one or more standby power supplies. Where available a building emergency power supply can be considered as an acceptable source of standby power provided it meets the requirements in Table 2.

The operating load conditions of the standby power supply are calculated on the following basis:

a) The nominal power consumption of the EACS equipment.

b) The expected number of operations (opening and closing) per hour for each access point with a fail-secure type actuator (i.e. those requiring power to open the access point).

c) The expected maximum number of fail-secure type actuators energised simultaneously and the anticipated peak load requirements of the system.

d) Each access point with fail-safe type actuators is constantly energised (i.e. those requiring power to keep the access point closed).

Refer to Annex B's standby battery capacity calculations as an example.

The EACS shall not prevent the free egress granted by other emergency systems (e.g. fire alarm).

8.2.2 Cabling

Cable routes should be selected to provide the shortest practical distance between the equipment locations. Care shall be taken to ensure the existing building fire rating is maintained where cables are routed through building structures.

Consideration should be given to the possibility of future expansion of the system and any likely changes to the building/site.

Cable types should be selected to minimise voltage drop and signal loss and comply with environmental, safety and security specifications. Current carrying capacities should not be exceeded and wherever possible adequate safety margins provided.

Cables should be installed within security controlled areas and wherever practicable should be concealed or not easily accessible.

Appropriate protection should be provided where cables are subjected to risk of physical damage or deliberate interference. If the risk of physical damage exists the cable should be mechanically protected, e.g. by ducting, trunking or conduit. When these are made of conductive material due regard should be paid to their proper electrical earthing and correct grounding.

Cables connecting parts of the EACS should be physically protected against tampering when run through areas having a lower security grade.

Open or short circuit conditions applied to wires connected to any components of an access control system installed outside its security controlled area or accessible from outside its security controlled area shall not result in the operation of the access point actuator allowing access to the secured area. Where it is required for the operation of the access point to be under the direct control of the emergency evacuation system (e.g. fire alarm) the integrity of the interconnection should be commensurate with the security level required by the grade of the EACS.

The power supply to each component of an EACS installed outside its controlled area shall be protected against short circuit conditions.

Extra low voltage and signal cables should not run in close proximity to mains or cables which might generate electrical interference.

9 Commissioning and system handover

9.1 Commissioning

The aim of the commissioning process is to confirm that the installed system meets the requirements of the system design.

The commissioning procedure should be agreed in writing between the system owner of the system and other interested parties.

A thorough visual inspection should be made to ensure that the installation, methods, materials, and components used comply with the system design guidelines in 7.3 and that the as-built documentation (including recorded drawings, operating instructions and agreed exceptions) corresponds to the actual installation.

When the system implementation is completed, but before handover, a competent person should inspect and verify that the system operates correctly and particularly that:

a) access points are functioning;
b) information given by the processing components is correct;
c) indication and annunciation is functioning correctly;
d) any connections to other systems are in operation and messages are correctly understood by the other systems;
e) the different types of annunciation operate correctly;
f) the relevant documents and instructions have been provided;
g) the system continues to work when the mains is disconnected (where standby power features are provided).

The commissioning and verification process does not need to include real customer data entry. Tests may be made with temporary data.

9.2 System handover

The system handover is to formally transfer the responsibility from the design and installation companies to the system owner. It is recommended that the conditions of the system handover be clearly defined between these parties.

A full demonstration of the EACS should be provided and the following aspects taken into account:

a) documentation (see Clause 11);
b) training in system management and operation.

After completion of the system handover the EACS should be tested for a period of time to be agreed with the system owner. During this period the EACS should be operated normally.

It is also possible that the test period is conducted as part of the commissioning and verification process prior to the handover.

On completion of the handover, the system owner should be made aware of changes between the system design and the as-built system and should be asked to sign an acceptance certificate stating the EACS has been installed and operates in accordance with the as-built documentation and that sufficient instruction and training has been provided to ensure the proper operation of the EACS.

10 System operation and maintenance

10.1 System operation

It should be the responsibility of the system owner to ensure that:

a) users and operators are trained;
b) instructions are provided for users and operators;
c) users are instructed and motivated about site security;
d) system administration and data back-up procedures are followed;
e) system data is updated;
f) the correct response is provided to any alert;
g) applicable national regulatory requirements are fulfilled;
h) regular maintenance of the system is organized;

i) organisational measures are in place in the event of failures of the EACS.

The installation/maintenance company should advise the system owner of his management responsibilities.

10.2 System maintenance

To ensure the EACS continues to function correctly, it should be inspected and serviced at agreed intervals, e.g., two times a year or if remote diagnostics are available the inspection and service interval can be reduced to once a year.

It is recommended that the arrangements for maintenance should be made before the EACS is put into operation.

A maintenance service level agreement should be made with a competent organization for inspection and servicing. Maintenance should only be carried out by persons properly trained and competent in the activities required for inspection and servicing of the system.

Different types of maintenance arrangements may be used, for example:

a) inspection procedure(s) – action limited to a diagnostic check of the system;
b) servicing procedure(s) – inspection followed by the repair or replacement of malfunctioning parts of the system

During maintenance work it might be necessary to operate the EACS in a degraded mode.

In all cases service personnel should notify the system operator and get clearance to proceed with the maintenance work. It is necessary to ensure that at the end of the maintenance work the full operation of the EACS is restored.

Inspection and servicing procedure(s) should be provided and documented by the component manufacturer or the installer. Inspection and service should be performed by the competent organization according to these procedures and include the inspection of operation of the access points.

In the event of any indication of malfunction (or possible future malfunction) of the system, or damage to any part of the system, the competent organization for inspection and servicing should be informed immediately.

The maintenance service level agreement should state the type and quantity of spare parts to be held and the ownership of these parts so that the agreed level of operation can be maintained.

A system record should be provided to record all system malfunctions, maintenance actions and details of any modifications or additions to the EACS.

11 Documentation

11.1 General

The level of documentation necessary for installation, operation, commissioning and maintenance of the EACS should reflect the size and complexity of the installed system and be provided in a language agreed with the system owner.

11.2 Documentation for planning

The documentation for the proposed installation should clearly identify:

a) the security controlled area(s);

b) the location of the recognition equipment(s);

c) the classification of each access point;

d) the location of the management equipment;

e) the connections to be established between the different components of the system.

Depending upon the size and complexity of the installation, specific information may be required covering:

1) cables routes;

2) interconnection details;

3) system schematics;

4) product literature.

11.3 Documentation for commissioning/system handover

The as-built documentation should be produced based upon the system design proposal and amended to include any changes to the EACS design found to be necessary during the installation process so that it describes the exact status of the EACS installed.

The as-built documentation should include information relating to the:

a) description of the installed system;

b) location of the system components;

c) relevant cable routes;

d) detailed interconnection drawings;

e) configuration settings.

The following documentation should be provided to the system owner. The system owner should be requested to make this documentation available should the EACS require modification, repair or maintenance. The system owner should also ensure the documentation is kept up to date:

1) as-built documentation;

2) system operating instructions;

3) system and component manuals;

4) installer/service provider contact details.

11.4 Documentation for maintenance

The documentation should include instructions for preventive maintenance, standby battery replacement intervals and for the inspection routine of the installed system.

Annex A
(normative)

Allowed exceptions for installed systems

A.1 General

This standard states that the installed EACS shall meet the grade dependent requirements given within IEC 60839-11-1 but 7.3.1 permits some application-specific exceptions for these requirements.

The requirements given in IEC 60839-11-1 are primarily intended for manufactured EACS and as such do not exactly match the requirements expected for EACS as installed.

Annex A provides information about the allowed exceptions from the graded requirements of IEC 60839-11-1 as considered to be most suitable for practice.

Reference to Annex A may be made by installers, customers, specifiers and end-users to reduce the need to document and explain the reasons for the exceptions.

All exceptions shall be agreed between the installer and the end-user and be recorded in the as-built documentation. The installer should point out how these exceptions may affect the functions and security of the EACS.

A.2 Claims of compliance

Claims of compliance in accordance with this part of IEC 60839 shall include reference to implemented exceptions as allowed by Annex A.

A.3 Allowed exceptions

If a function is provided it shall meet the applicable requirements of the grade for which compliance is claimed.

The followingTables A.1 to A.8 list the allowed exceptions (shown in ***bold italics***) applicable only to an installed EACS.

NOTE The line numbers in the tables below correspond to the line numbers in the respective tables of IEC 60839-11-1.

Table A.1 – Allowed exceptions for access point interface requirements

Access point interface requirements (IEC 60839-11-1:2013, 6.2, Table 2)		Grade assignment			
		1	2	3	4
6	Provide access control for exit from a protected (controlled) area	OP	***OP***	***OP***	M
7	Hard anti-passback	OP	OP	***OP***	M
16	Dual occupancy (two or more persons presence check)	OP	OP	OP	***OP***
17	Dual access (two-person access)	OP	OP	OP	***OP***

Table A.2 – Allowed exceptions for indication and annunciation requirements

Indication and annunciation requirements (IEC 60839-11-1:2013, 6.3, Table 3)					Grade assignment			
					1	2	3	4
A – Portal (local indication)								
		Indication						
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	***OP***	***OP***
B – Monitoring console (annunciation)								
		Display	Alert	Logging				
6	Logging is required when access is granted			•	OP	OP	***OP***	M
7	Visual annunciation, alert and logging required for duress conditions. Duress signalling is not mandatory. When duress signalling is provided, visual annunciation, alert and logging for duress condition is required.	•	•	•	OP	OP	OP	***OP***
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	***OP***	M
17	Access denied. It may be configurable by portal in accordance with the grade requirement. It is mandatory for installations of grades 3 and 4 EACS to have enabled the display, alert and logging of the access denied events.	•	•	•	OP	OP	M	M
25	Roll call	•		•	OP	OP	***OP***	***OP***
35	*Reader* condition off-line	•	•	•	OP	OP	OP	***OP***
37	Annunciation of reaching the limit of 90 % from maximum logging capacity. It is recommended that installers refer to manufacturer information and to inform the end-user whether this information is of importance and under what conditions it would occur.	•	•	•	OP	OP	M	M
41	System shall be capable of assigning priority levels to specific alert events	•			OP	OP	***OP***	***OP***

Table A.3 – Allowed exceptions for recognition requirements

Recognition requirements (IEC 60839-11-1:2013, 6.4, Table 4)		Grade assignment			
		1	2	3	4
	A – Access levels				
6	Minimum number of user access levels NOTE The minimum number is undefined.	***OP***	***OP***	***OP***	***OP***
7	Minimum number of configurable time periods NOTE The minimum number is undefined.	***OP***	***OP***	***OP***	***OP***
9	Minimum resolution for time within access level includes day of month, month and year	N/A	OP	OP	***OP***
24	Support for multiple facility codes if the system utilizes facility coding	OP	OP	OP	***OP***

Table A.4 – Duress signalling requirements

Duress signalling requirements (IEC 60839-11-1:2013, 6.5, Table 5)	Grade assignment			
	1	2	3	4
Duress signalling is not mandatory. When duress signalling is implemented it shall fulfil the requirements in IEC 60839-11-1:2013, Table 5.				

Table A.5 – Overriding requirements

Overriding requirements (IEC 60839-11-1:2013, 6.6, Table 6)	Grade assignment			
	1	2	3	4
No exceptions are allowed.				

Table A.6 – Communication requirements

Communication requirements (IEC 60839-11-1:2013, 6.7)	Grade assignment			
	1	2	3	4
No exceptions are allowed.				

Table A.7 – Allowed exceptions for system self-protection requirements

System self-protection requirements (IEC 60839-11-1:2013, 6.8, Table 7)		Grade assignment			
		1	2	3	4
12	The minimum number of required characters for logical access by memorized information only shall be as indicated (N=numeric/A=alphanumeric). This requirement applies to access to the system for the purposes of configuration. The requirement does not therefore conflict with recognition requirements in IEC 60839-11-1:2013, Table 4.	4N	5N	6A	8A
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). Exception: the system should not prevent individuals from changing their own memorized information.	OP	OP	M	M
15	Logical access credential can only be assigned by the system administrator. Exception: the system should not prevent individuals from changing their own memorized information.	OP	OP	M	M
18	Encryption required for communication signals between components of the EACS when using publicly shared networks (e.g. the Internet).	OP	OP	M	M

System self-protection requirements (IEC 60839-11-1:2013, 6.8, Table 7)		Grade assignment			
		1	2	3	4
	NOTE The use of a Virtual Private Network is not considered to be a publicly shared network.				
19	The information stored on the token shall be protected against unauthorized modification or reproduction. (For grade 3 only): when the requirement above cannot be met consideration should be given to the use of a combination of two or more recognition methods.	OP	OP	M	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. Note that at grade 4 it is mandatory to comply with item 24. At grade 3 it is mandatory for manufacturers to comply with item 24 or item 25 (or both). Installers should follow installation requirements stated by manufacturers if compliance is by way of item 25.	OP	OP	OP*	OP

Table A.8 – Allowed exceptions for power supply requirements

Power supply requirements (IEC 60839-11-1:2013, 6.9, Table 8)	Grade assignment			
	1	2	3	4
For allowed exceptions refer to 8.2.1, Table 2.				

Annex B
(informative)

Standby battery capacity calculations

The minimum standby battery capacity can be calculated as shown:

Measure	Unit	Description	Example
n_i	Per hour	Expected number of actuations per hour (opening and closing of a portal) per portal	150, 30, ...
t_{acti}	Seconds	Duration of one actuation for a fail-secure actuator	2, 5, ...
I_{equip}	Amperes	Power consumption of EACS equipment (excluding actuators)	0,5
$I_{fail\text{-}secure}$	Amperes	Power consumption of all fail-secure actuators (in activated state)	2
$I_{fail\text{-}safe}$	Amperes	Power consumption of all fail-safe actuators (in activated state)	3
t	Hours	Required standby time	2
D_i	%	Duty cycle (percentage of time of actuations per hour) per portal	
I_{avg}	Amperes	Average load for expected load conditions	
C	Ah	Required minimum battery capacity	

$D_i = t_{acti} \times n_i / 3\,600$	Example: $D_1 = 2 \times 150/3\,600$ $D_1 = 8{,}33$ % $D_2 = 5 \times 30/3\,600$ $D_2 = 4{,}17$ %

$I_{fail\text{-}safe} = I_{fail\text{-}safe1} + I_{fail\text{-}safe2} + \ldots$ $I_{fail\text{-}secure} = I_{fail\text{-}secure1} \times D_1 + I_{fail\text{-}secure2} \times D_2 + \ldots$	Example: $I_{fail\text{-}safe} = 0{,}5 + 0{,}3 + \ldots = 3$ A $I_{fail\text{-}secure} = 0{,}4 \times 0{,}083\,3 + 0{,}6 \times 0{,}041\,7 + \ldots = 0{,}17$ A

$I_{avg} = I_{equip} + I_{fail\text{-}secure} + I_{fail\text{-}safe}$	Example: $I_{avg} = 0{,}5 + 0{,}17 + 3$ $I_{avg} = 3{,}67$ A

$C = t \times I_{avg}$	Example: $C = 2 \times 3{,}67$ $C = 7{,}34$ Ah
Battery selection NOTE Taking into account the de-rating factor derived from the manufacturer's specifications.	Assume a 20 % de-rating factor $C = 7{,}34 \times 1{,}2$ $C = 8{,}8$ Ah Therefore select a battery with minimum capacity greater than 8,8 Ah (in this case a standard value for the battery capacity might be 10 Ah).

When choosing the battery capacity it is recommended that a de-rating factor be introduced taking into account the battery manufacturer's specifications (for example, the battery type, the effects of aging, the operating temperature, etc.).

Bibliography

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*

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*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC 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 IEC 60839-11-2 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/476/FDIS	79/489/RVD

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

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

Une liste de toutes les parties de la série IEC 60839, publiées sous le titre général *Systèmes d'alarme et de sécurité électroniques*, peut être consultée sur le site web de l'IEC.

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 l'IEC 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 de la série IEC 60839 écrite pour inclure 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 l'IEC 60839 décrit les exigences générales concernant la planification, l'installation, le fonctionnement, la maintenance et la documentation de l'application des systèmes de contrôle d'accès électronique (EACS[1]).

Les performances des EACS sont déterminées par les classes de sécurité allouées aux points d'accès. Il convient en premier lieu d'effectuer une évaluation des risques qui identifie les risques et les menaces perçues afin d'établir les classes de sécurité appropriées.

Quatre classes de sécurité sont disponibles sur la base du degré de connaissance et des outils disponibles en matière de tentative d'accès par des personnes non autorisées et en fonction du type d'application, en tenant compte des aspects organisationnels spécifiques et de la valeur des biens.

Des lignes directrices distinctes sont prévues pour chaque activité ainsi que des recommandations pour la documentation nécessaire. Une brève description de chaque section portant sur les activités est fournie ci-dessous:

Planification du système: cette section est destinée à aider le concepteur dans le choix d'un système de contrôle d'accès électronique (EACS) qui assure le contrôle de l'accès et l'intégrité de la sécurité en rapport avec la valeur des biens nécessitant une protection et les risques associés. Voir l'Article 7.

Il convient que la conception du système permette de réduire au minimum les vulnérabilités éventuelles qui pourraient être exploitées pour contourner les mesures de contrôle d'accès. Il est recommandé d'intégrer des protections permettant de déclencher des alertes précoces sur les tentatives de contournement des mesures de contrôle d'accès. Voir 7.3.

Installation du système: cette section vise à aider les responsables de l'installation des EACS en identifiant les questions qu'il convient de prendre en considération avant le démarrage de l'installation et lors de l'installation du système afin de garantir une mise en œuvre correcte de l'EACS, telle que spécifiée lors de la planification du système. Voir l'Article 8.

Mise en service et mise à disposition du système: cette section fournit des lignes directrices permettant de s'assurer que le niveau de performance exigé lors de la planification du système est obtenu et que l'utilisateur final reçoit la documentation nécessaire, les enregistrements et les consignes d'utilisation au cours de la mise à disposition de l'EACS. Voir l'Article 9.

Fonctionnement et maintenance du système: cette section inclut les informations relatives aux responsabilités de l'utilisateur final de l'EACS à s'assurer que le système fonctionne correctement et est convenablement entretenu. Elle porte sur l'inspection, l'entretien et l'utilisation de diagnostics à distance afin de pouvoir maintenir le niveau de performance déterminé à la phase de planification du système. Voir l'Article 10.

---

1 EACS = *Electronic access control systems*.

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

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

1 Domaine d'application

La présente partie de l'IEC 60839 définit les exigences et les lignes directrices minimales concernant l'installation et le fonctionnement des systèmes de contrôle d'accès électronique (EACS) et/ou des équipements annexes pour satisfaire à différents niveaux de protection.

La présente norme inclut des exigences en matière de planification, d'installation, de mise en service, de maintenance et de documentation pour l'application d'EACS installés à l'intérieur et autour des bâtiments et des zones. Les fonctions des équipements sont définies dans l'IEC 60839-11-1.

Lorsque l'EACS inclut des fonctions relatives au hold-up ou à la détection d'intrus, les exigences des normes relatives à l'intrusion et au hold-up sont également applicables.

La présente norme fournit des lignes directrices d'application destinées à aider les personnes responsables de l'établissement des EACS afin d'assurer l'adéquation de la conception et de la planification de l'EACS, à la fois en termes de niveaux de protection et de niveaux de performance nécessaires pour fournir le niveau de contrôle d'accès et de protection jugé approprié pour chaque installation. Ceci est obtenu par la mise à l'échelle ou la classification des caractéristiques des systèmes de contrôle d'accès électronique liées à la fonctionnalité de sécurité (par exemple la reconnaissance, l'activation des points d'accès, le contrôle du point d'accès, le signalement d'agression et l'autoprotection des systèmes) en conformité avec les conditions de menaces connues ou perçues.

La présente norme ne traite pas des méthodes ni des procédures de réalisation d'une évaluation des risques.

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).

IEC 60839-11-1:2013, *Systèmes d'alarme et de sécurité électroniques – Partie 11-1: Systèmes de contrôle d'accès électronique – Exigences système et exigences concernant les composants*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 60839-11-1, ainsi que les suivants, s'appliquent.

3.1
région
partie d'une zone protégée, qui a son propre ensemble de niveaux d'accès

Note 1 à l'Article: Elle peut avoir une classe de sécurité différente de celle d'autres régions dans la même zone protégée.

3.2
organisme compétent
organisme possédant suffisamment de ressources et du personnel bien expérimenté et bien formé pour la maintenance des EACS

3.3
à sécurité intrinsèque
à ouverture intégrée
dispositif de verrouillage conçu de manière à se relâcher automatiquement en cas de panne d'alimentation

3.4
à fermeture intégrée
à verrouillage intégré
dispositif de verrouillage conçu de manière à rester fermé en cas de panne d'alimentation

3.5
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 ou accès contrôlés

Note 1 à l'Article: Elle peut contenir plusieurs régions individuelles avec des classes de sécurité similaires ou différentes. Se reporter à la définition de "Région" en 3.1.

3.6
propriétaire du système
personne ou groupe de personnes qui prend la décision de ce qui est approprié pour les locaux respectifs à utiliser en vue d'obtenir le contrôle d'accès / la protection / le prix / etc. souhaités

4 Abréviations

Pour les besoins du présent document, les abréviations de l'IEC 60839-11-1, ainsi que les suivantes, s'appliquent.

ACU Access control unit *(Unité de contrôle d'accès)*

EACS Electronic access control system *(Système de contrôle d'accès électronique)*

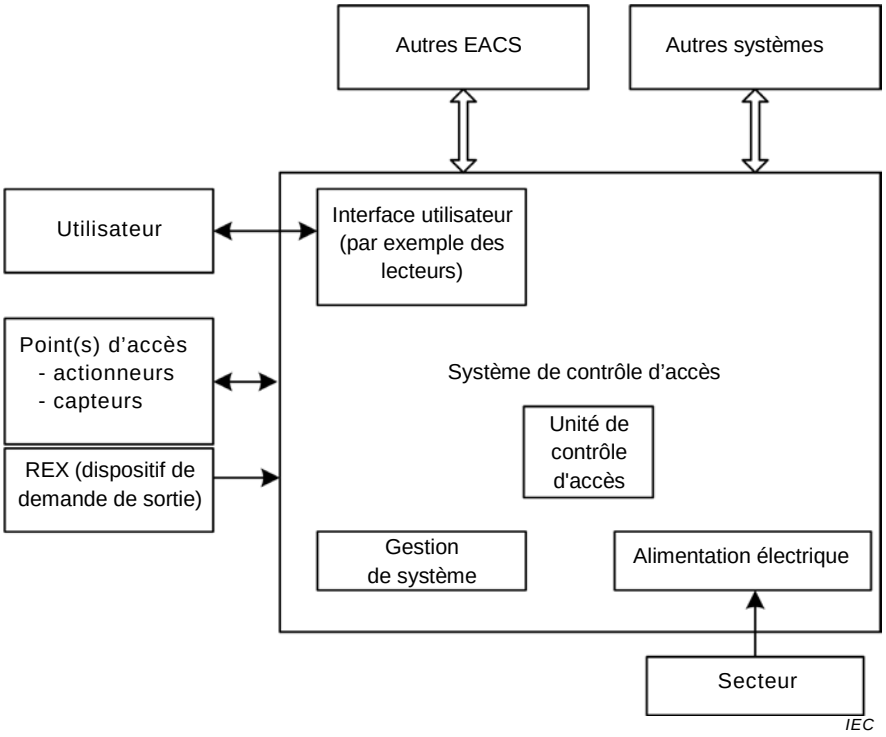
EMC Electromagnetic compatibility *(Compatibilité électromagnétique)*

REX Request to exit *(Dispositif de demande de sortie)*

5 Architecture système

Un système de contrôle d'accès comprend toutes les infrastructures de construction et d'organisation ainsi que les équipements exigés pour le contrôle d'accès. La Figure 1 est un exemple de disposition typique des composants et des interfaces d'un EACS.

Il convient que la protection physique et la résistance mécanique des actionneurs, des capteurs, etc., soient compatibles avec la classe de sécurité de chaque point d'accès. Il convient de tenir compte de la résistance physique des constructions voisines (par exemple les murs, les portes, etc.).



L'IEC 60839-11-1:2013, Tableau 8, indique que: "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" exigée conformément à la classe de sécurité de l'EACS. Il est recommandé que des sources d'alimentation de secours contrôlées soient fournies à tous les actionneurs et aux consoles de commande.

Figure 1 – Disposition typique des composants et des interfaces d'un EACS

6 Considérations concernant l'environnement et la CEM

6.1 Généralités

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. Les composants doivent être adaptés à une des classes d'environnement suivantes.

6.2 Classe d'environnement I – Equipements situés à l'intérieur mais limités à un environnement résidentiel ou à des bureaux

La classe d'environnement I comprend les influences d'environnement normalement expérimentées à l'intérieur lorsque la température est bien maintenue (par exemple dans un bâtiment de type résidentiel ou commercial).

NOTE On peut s'attendre à une variation de température entre +5 °C et +40 °C.

6.3 Classe d'environnement II – Equipements situés à l'intérieur – En général

La classe d'environnement II comprend les influences d'environnement normalement expérimentées à l'intérieur lorsque la température n'est pas bien maintenue (par exemple dans les couloirs, les halls ou les escaliers et où une condensation peut se produire sur les fenêtres et dans les aires de stockage non chauffées ou dans les entrepôts où le chauffage est intermittent).

NOTE On peut s'attendre à une variation de température entre –10 °C et +55 °C.

6.4 Classe d'environnement III – Equipements situés à l'extérieur – Sous abri ou à l'intérieur avec des conditions extrêmes

La classe d'environnement III comprend les influences d'environnement normalement expérimentées à l'extérieur lorsque les composants de l'EACS ne sont pas pleinement exposés aux intempéries, ou expérimentées à l'intérieur lorsque les conditions d'environnement sont extrêmes.

NOTE On peut s'attendre à une variation de température entre –25 °C et +55 °C.

6.5 Classe d'environnement IV – Equipements situés à l'extérieur – En général

La classe d'environnement IV comprend les influences d'environnement normalement expérimentées à l'extérieur lorsque les composants de l'EACS sont pleinement exposés aux intempéries.

NOTE On peut s'attendre à une variation de température entre –25 °C et +70 °C selon la zone. La plage de températures peut être étendue vers le haut et/ou vers le bas pour différentes zones géographiques ou climatiques.

6.6 CEM

Il est recommandé de suivre de bonnes techniques d'installation pour réduire les effets indésirables des interférences électriques. Il convient par exemple de ne pas faire passer les câbles d'interconnexion dans le même conduit ou dans le même tube que les câbles transportant l'alimentation secteur ou que les câbles réseau ou de données transportant des signaux haute fréquence sauf s'ils sont séparés physiquement et/ou correctement protégés par un écran pour empêcher les interférences croisées.

Une protection et/ou un filtrage supplémentaires des câbles d'interconnexion peuvent être nécessaires pour les applications de niveau élevé d'interférences électriques conduites ou rayonnées, par exemple une installation industrielle faisant fonctionner des équipements électriques de forte puissance.

Il convient de suivre les lignes directrices des fabricants en ce qui concerne la compatibilité électromagnétique.

7 Planification du système

7.1 Généralités

La phase de planification du système a pour objectif de déterminer l'étendue de l'EACS, de sélectionner les éléments des critères de fonctionnalité/performances appropriés, la classe de sécurité et la classe d'environnement et d'élaborer un projet de conception du système.

Un système de contrôle d'accès comprend toutes les fonctionnalités logiques, les infrastructures de construction et d'organisation ainsi que les équipements physiques nécessaires pour contrôler l'accès.

Il convient de veiller particulièrement à réduire au minimum les désagréments pour les utilisateurs autorisés.

Il convient de mettre en œuvre un système de contrôle d'accès conformément à la séquence suivante:

a) évaluation des risques et classification de la sécurité;

b) choix du système et des composants;

c) considérations d'ordre opérationnel;

d) installation du système;

e) mise à disposition du système;

f) fonctionnement et maintenance du système.

L'installation du système doit être effectuée conformément aux règlementations nationales et locales.

7.2 Evaluation des risques et classification de sécurité

Il est indispensable de réaliser une évaluation des risques avant la mise en œuvre du système de contrôle d'accès. La représentation graphique de l'évaluation des risques de la Figure 2 présente les principales considérations.

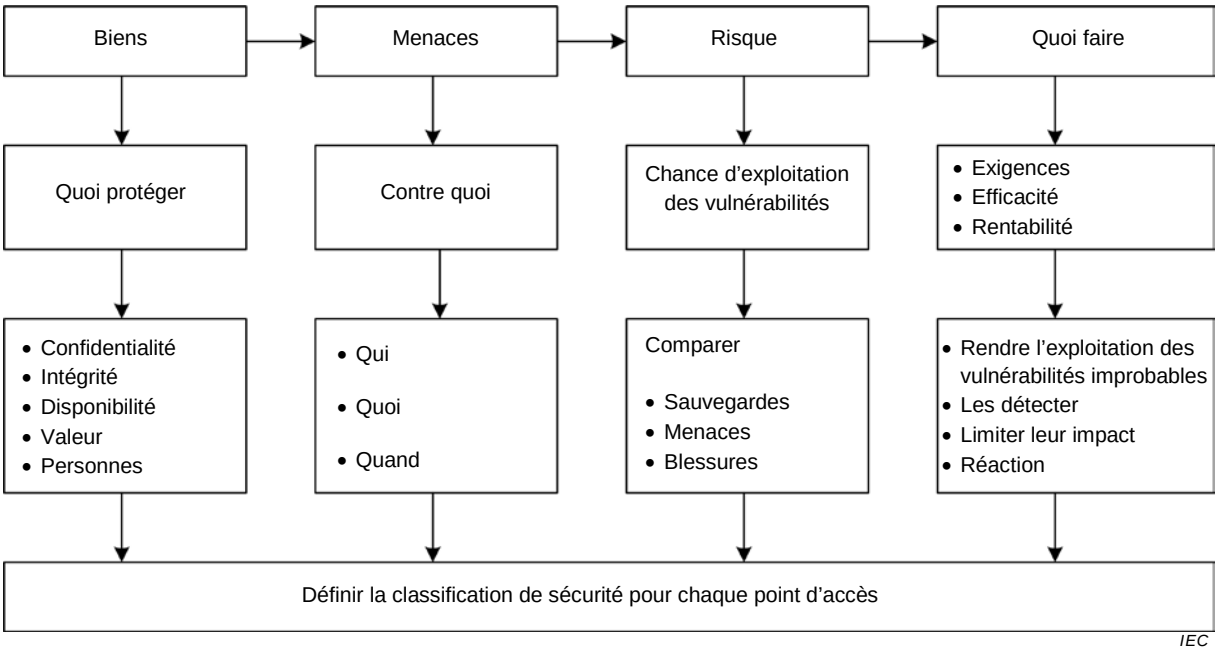


Figure 2 – Représentation graphique de l'évaluation des risques

Les niveaux de classes de sécurité 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 (malfaiteurs). Le Tableau 1 donne des exemples d'applications typiques pour chaque classe.

– Classe 1: risque faible. Le malfaiteur est supposé mal connaître le système de contrôle d'accès et être limité à une gamme restreinte d'outils facilement disponibles. La sécurité physique est fournie en vue de décourager et de retarder les malfaiteurs. Les biens ont une valeur limitée et les malfaiteurs abandonneront vraisemblablement toute idée d'agression lorsqu'ils seront confrontés à une résistance minimale.

– Classe 2: risque faible à moyen. Le malfaiteur 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 est fournie en vue de décourager, retarder et détecter les malfaiteurs. Les biens ont une plus grande valeur et les malfaiteurs sont susceptibles d'abandonner toute idée de réussite lorsqu'ils s'apercevront qu'ils peuvent être détectés.

– Classe 3: risque moyen à élevé. Le malfaiteur 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 est fournie en vue de décourager, retarder, détecter les malfaiteurs et des moyens sont fournis pour faciliter l'identification des malfaiteurs. Les biens ont une grande valeur et les malfaiteurs peuvent abandonner toute idée de réussite lorsqu'ils s'aperçoivent qu'ils peuvent être identifiés et pris en flagrant délit.

– Classe 4: risque élevé. Le malfaiteur 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 est fournie en vue de décourager, retarder, détecter les malfaiteurs et des moyens sont fournis pour faciliter l'identification des malfaiteurs. Les biens ont une très grande valeur et les malfaiteurs peuvent abandonner toute idée de réussite lorsqu'ils s'aperçoivent qu'ils seront identifiés et pris en flagrant délit.

Tableau 1 – Classification de sécurité

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 malfaiteurs / agresseurs	Faible compétence, faible connaissance des EACS, aucune connaissance des technologies des jetons et des technologies de l'information. Ressources financières faibles pour les agressions	Compétence et connaissance moyennes des EACS, faible connaissance des technologies des jetons et des technologies de l'information. Ressources financières faibles à moyennes pour les agressions	Compétence et connaissance élevées des EACS, connaissance moyenne des technologies des jetons et des technologies de l'information. Ressources financières moyennes pour les agressions	Compétence et connaissance très élevées des EACS, connaissance élevée des technologies des jetons et des technologies de l'information. 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)

7.3 Conception du système

7.3.1 Choix du système et des composants

La classification de sécurité doit être définie pour chaque point d'accès, en prenant en considération les besoins de contrôle d'entrée et de sortie.

Différentes classes de sécurité peuvent être utilisées pour les points d'accès dans le même système. On doit s'assurer que les composants de système communs, assurant la protection des points d'accès avec différentes classes de sécurité, répondent aux exigences du point d'accès avec la classe de sécurité la plus élevée qu'ils exploitent ensemble (voir Figure 3).

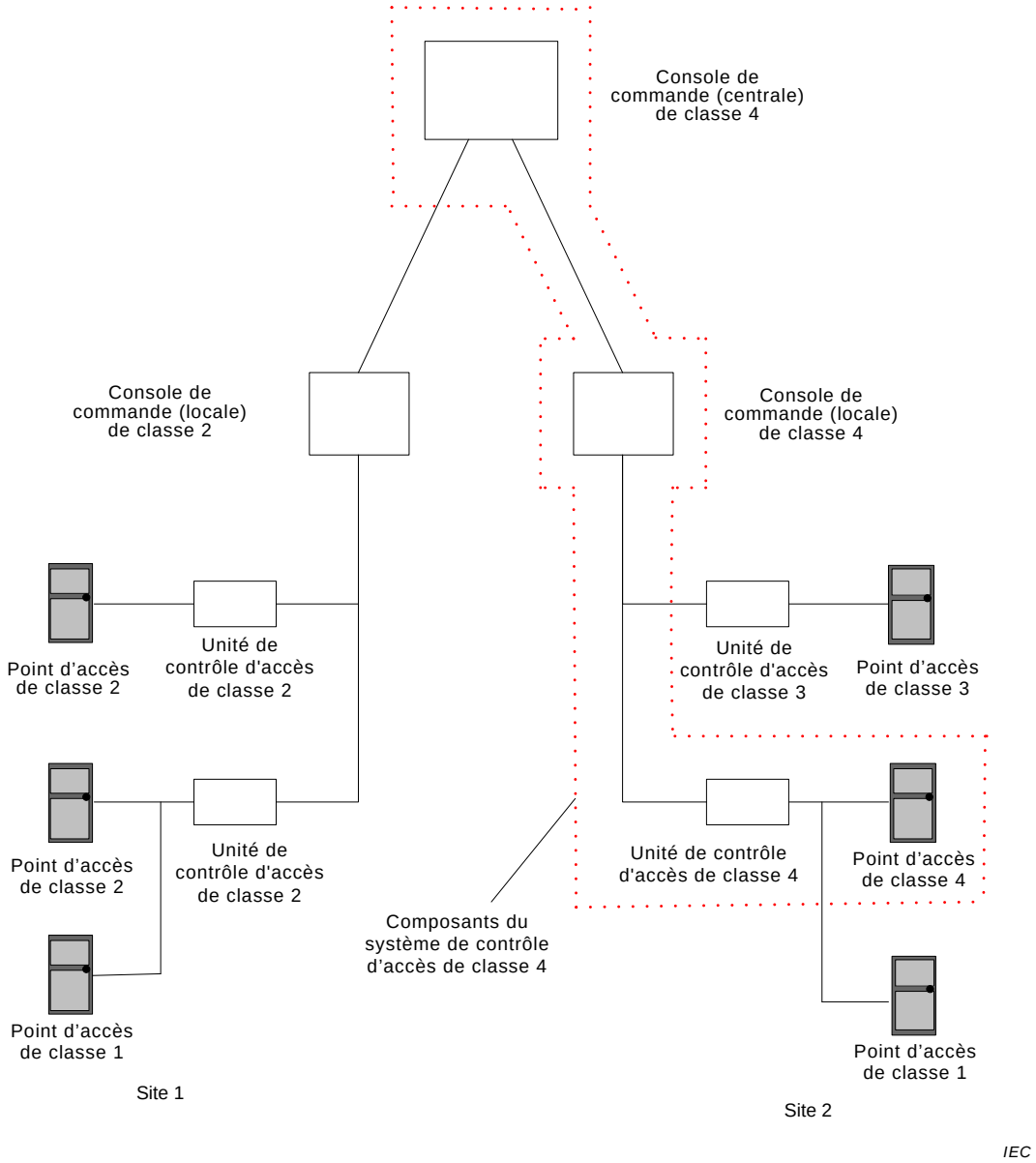


Figure 3 – Exemple de choix de la classe de système

Lorsqu'il n'est pas pratique d'avoir différentes classes de points d'accès gérées par un système unique de contrôle d'accès, il est permis d'avoir plus d'un système de contrôle d'accès individuel. Un point d'accès ne doit pas être contrôlé par plus d'un système de contrôle d'accès individuel.

Les fonctions obligatoires de l'équipement associé à chaque classe de sécurité sont définies dans l'IEC 60839-11-1.

Il n'est pas nécessaire de mettre en œuvre toutes les fonctions obligatoires définies dans l'IEC 60839-11-1 dans un EACS installé. L'Annexe A donne une liste des exceptions autorisées. Les exceptions doivent faire l'objet d'un accord entre l'installateur et le propriétaire du système et être consignées dans la documentation du système conforme à l'exécution.

L'installateur doit signaler au propriétaire du système que les exceptions par rapport aux exigences, notamment pour les points d'accès, la reconnaissance et la communication, peuvent avoir une incidence sur les fonctions et la sécurité de l'EACS dans son ensemble.

7.3.2 Considérations d'ordre opérationnel

7.3.2.1 Généralités

Les considérations d'ordre opérationnel dans ce paragraphe sont des lignes directrices concernant les points de discussion avec le client afin de comprendre et de répondre aux besoins de l'installation finale.

Ces lignes directrices sont également à examiner conjointement avec les fonctions obligatoires pour chaque classe de sécurité de l'EACS comme cela est spécifié dans l'IEC 60839-11-1.

Les lignes directrices ne sont pas exhaustives et ne sont pas énumérées dans un ordre de priorité.

7.3.2.2 Lignes directrices

Il convient de prendre en considération les points suivants:

a) les recommandations du fabricant;
b) la ou les menaces;
c) les biens spécifiques nécessitant une protection;
d) les activités menées au niveau du site/bâtiment;
e) la philosophie des mesures de contrôle d'accès;
f) la classe de sécurité pour chaque point d'accès;
g) le flux d'utilisateurs (nombre de personnes pendant un laps de temps);
h) le fonctionnement du système de contrôle d'accès en cas de panne (par exemple la nécessité d'une seconde source d'alimentation, l'infrastructure des câbles des équipements, la perte de communication, etc.);
i) le contrôle d'accès pour les utilisateurs handicapés;
j) les exigences en matière de sécurité (par exemple les issues de secours, la protection contre les incendies, etc.);
k) les conditions d'environnement et de CEM du site;
l) la redondance, les plans de reprise après sinistre pour la console de commande;
m) l'emplacement des équipements (unité de contrôle, interface utilisateur, console de commande);
n) la coopération des utilisateurs (motivation, formation, etc.);
o) la formation des opérateurs;
p) les chemins de câble, le type de câble, la longueur maximale de câble;
q) les liaisons de communication (disponibilité, fiabilité, sécurité, performances);
r) la détection des violations;
s) la méthode d'établissement des rapports sur les alarmes/alertes;
t) le flux de personnes (personnel et visiteurs);
u) la gestion des visiteurs;
v) les dispositions des forces d'intervention (par exemple la police);
w) l'accès des véhicules;
x) les niveaux d'accès (autorisation) pour chaque région.

7.3.2.3 Exigences réglementaires

Il convient d'accorder une attention particulière à toutes les exigences internationales, nationales ou locales applicables, y compris:

a) les mesures pour les personnes handicapées;

b) les lois relatives à la protection des données et de la vie privée;

c) les réglementations spécifiques au secteur;

d) les questions de santé et de sécurité, l'évacuation en toute sécurité dans des situations d'urgence.

7.3.2.4 Reconnaissance

Il convient de considérer, au moment du choix des équipements et méthodes de reconnaissance, les points suivants:

a) l'aptitude de l'équipement de reconnaissance pour l'application spécifique, y compris la commodité d'utilisation, le flux d'utilisateurs prévu, l'environnement d'exploitation et la durée de vie prévue des équipements, etc.;

b) les méthodes de reconnaissance, par exemple l'utilisation d'un code PIN seul, d'un jeton/carte seul, de la biométrie ou d'une combinaison de méthodes (c'est-à-dire une méthode multifactorielle).

7.3.2.5 Gestion du système

Pour assurer la continuité et la fiabilité du fonctionnement de l'EACS, une gestion adéquate de système est exigée et il convient de prendre en considération, le cas échéant, les éléments suivants:

a) l'exploitation et les obligations vis-à-vis du système (programmation, gestion des identifiants, administration des droits d'accès, configuration, gestion des alarmes jour et nuit);

b) les compétences et la formation des opérateurs de système;

c) l'établissement de rapports;

d) l'archivage et la politique de sauvegarde;

e) le nombre d'utilisateurs et de niveaux d'accès en tenant compte à la fois des besoins présents et des besoins futurs prévus;

f) la facilité d'utilisation (utilisateur, gestion, aptitude au service, etc.);

g) les exigences concernant l'annonce (par exemple un affichage, un enregistrement, une alerte, etc.);

h) la capacité de l'enregistreur chronologique;

i) la coordination des fonctions d'annonce (emplacement, procédures, présentation, etc.);

j) la neutralisation.

7.3.2.6 Points d'accès

Pour l'installation et le fonctionnement appropriés des points d'accès, il convient de prendre en considération les éléments suivants:

a) les exigences concernant l'indication;

b) le fonctionnement en cas de panne;

c) d'autres facteurs pertinents (par exemple le risque de vandalisme, etc.);

d) la force physique;

e) la structure du bâtiment avoisinant;

f) le choix d'actionneurs appropriés du point d'accès, c'est-à-dire des serrures, des barres de sûreté (niveau de sécurité, aspect, environnement d'exploitation, temps de réponse de fonctionnement, exigences concernant l'installation sur une structure existante);

g) les exigences en matière de sécurité (par exemple les issues de secours, la protection contre les incendies, etc.);

h) la surveillance du point d'accès;

i) la détection/prévention de deux personnes ou plus qui tentent une entrée simultanée (c'est-à-dire la singularisation);

j) la méthode de retour du point d'accès à l'état fermé (par exemple les équipements de fermeture automatique des portes);

k) la configuration du fonctionnement en cas de coupure de courant (sécurité intrinsèque, fermeture intégrée);

l) les mesures pour les personnes handicapées;

m) les mesures spécifiques pour la gestion des livraisons;

n) la classification de sécurité pour les points d'accès conduisant à la même zone de sécurité contrôlée;

o) les mesures de reconnaissance/détection supplémentaires (poids, détection des métaux, comparaison des images, inspection visuelle, etc.);

p) le dispositif anti-retour (logique, temporisé, zone contrôlée);

q) la neutralisation;

r) l'alarme d'agression;

s) les conditions d'accès pour deux utilisateurs;

t) le contrôle de présence.

7.3.2.7 Interface avec d'autres systèmes

Lorsqu'il est nécessaire d'interfacer l'EACS avec d'autres systèmes tels que des systèmes d'alarme anti-intrusion, des systèmes de vidéosurveillance, des systèmes d'administration, un interphone, un système de contrôle d'ascenseur, etc., il convient de prendre en considération les points suivants:

a) la nature des liaisons de communication, la disponibilité, la fiabilité et la sécurité souhaitées des données transmises associées à ces liaisons;

b) les exigences concernant l'infrastructure du réseau;

c) les commandes de fonctionnement spécifiques, par exemple pour l'appel de l'ascenseur, le choix de l'étage et de la destination;

d) les commandes d'établissement de rapports associées au système de contrôle d'ascenseur.

8 Installation du système

8.1 Généralités

Il convient de prendre en considération toutes les exigences applicables en matière de sécurité avant le démarrage des travaux.

Les méthodes d'installation électrique doivent être conformes aux règlementations locales des sites et nationales en vigueur.

Il convient que les composants de l'EACS soient installés dans des endroits qui garantissent une sécurité adéquate pour le fonctionnement et qui permettent un accès facile à des fins de maintenance et d'entretien.

Il convient que tous les composants du système correspondent aux conditions d'environnement dans lesquelles ils fonctionnent.

Il convient de prendre des précautions lors de la sélection des composants pour s'assurer que tous les composants du système sont compatibles. En cas d'incertitude, il convient de consulter de façon appropriée, par exemple avec le fabricant ou le fournisseur de composants, un laboratoire d'essai ou une autre tierce partie appropriée.

Les résultats de l'évaluation des risques doivent déterminer les classes de sécurité des régions à l'intérieur de la zone protégée. Les points d'accès à ces régions doivent être d'un niveau équivalent ou supérieur. Pour chaque région, des niveaux d'accès distincts peuvent être définis.

À l'exception de l'interface utilisateur, les équipements critiques pour l'intégrité de la sécurité du système de contrôle d'accès ne doivent pas être placés dans une région désignée comme ayant un niveau de sécurité inférieur au niveau le plus élevé de la zone protégée qu'ils contrôlent. Voir la Figure 4.

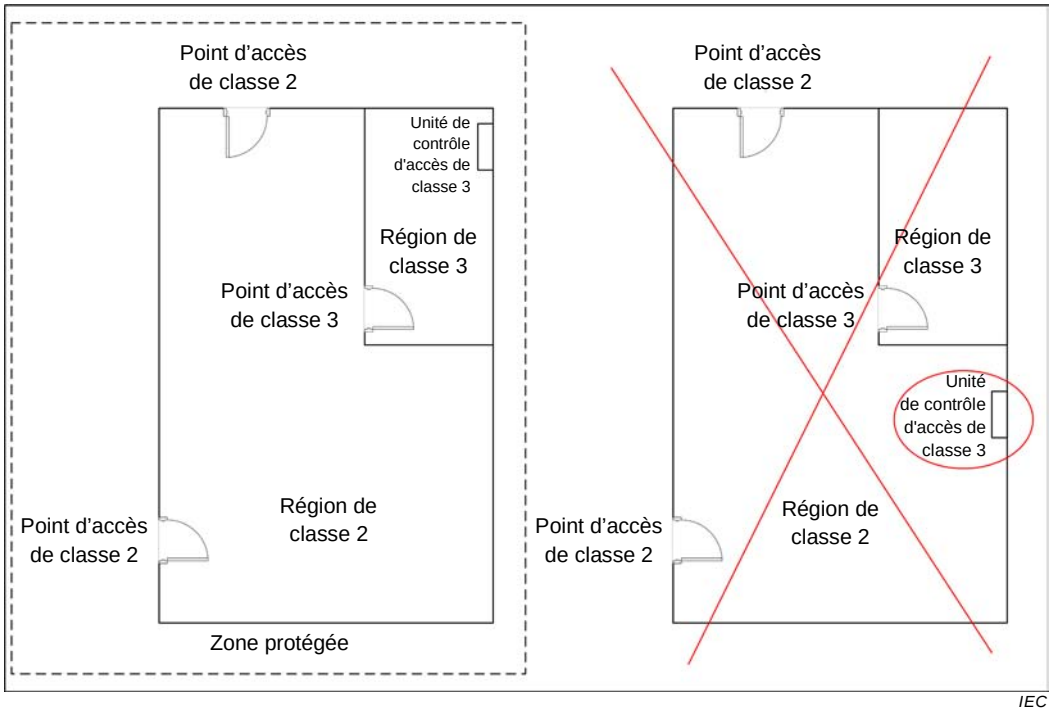


Figure 4 – Emplacement de l'équipement en fonction de la classe de sécurité de la zone protégée

L'installateur doit tenir le propriétaire du système informé des fonctionnalités spécifiques qui doivent être mises en œuvre afin de respecter les mesures d'organisation et de construction nécessaires au bon fonctionnement des EACS. Par exemple, la détection/prévention de deux personnes ou plus qui tentent d'entrer simultanément (singularisation) est recommandée pour la mise en œuvre des mesures anti-passage en double.

Il convient de prendre en considération le cheminement des câbles uniquement dans la zone protégée (voir 8.2.2).

8.2 Planification de l'installation

8.2.1 Equipements

Les équipements utilisés dans des installations couvertes par la présente norme doivent être conformes aux exigences de l'IEC 60839-11-1 relatives à la classe de sécurité et à la classification d'environnement applicables.

Il convient qu'un personnel bien formé installe les équipements conformément aux instructions du fabricant. S'il n'est pas possible d'installer un composant conformément aux recommandations du fabricant, il convient de demander conseil auprès du fabricant et il convient de le consigner dans la documentation du système conforme à l'exécution.

Lorsque l'EACS utilise l'infrastructure (réseau) de communication existante sur le site du client, il convient de veiller à s'assurer que des mesures suffisantes en termes de capacité, de performances et de protection sont en place pour permettre le bon fonctionnement de l'EACS pour la classe de sécurité sélectionnée.

Les boîtiers des composants d'un EACS doivent comporter des moyens qui empêchent tout accès non détecté aux éléments internes afin de réduire au minimum le risque de violation. Les exigences concernant l'inviolabilité peuvent varier en fonction de la classe de sécurité du système de contrôle d'accès électronique et en fonction de la position d'un composant du système à l'intérieur ou à l'extérieur de la zone de sécurité contrôlée.

Il convient de prendre des dispositions lors de la planification du système de contrôle d'accès pour permettre un accès contrôlé aux zones protégées en cas de dysfonctionnement ou de panne du système.

Il convient que les sources d'alimentation soient situées dans la zone de sécurité contrôlée. Lorsque cela n'est pas possible, il convient de prendre des mesures complémentaires pour maintenir un niveau de sécurité équivalent à la zone de sécurité contrôlée.

Il convient de choisir les caractéristiques assignées des alimentations de manière à répondre à la spécification électrique de chaque composant associé par rapport à la plus grande charge prévue dans des conditions normales de fonctionnement.

NOTE On parle de condition normale de fonctionnement lorsque tous les équipements de l'EACS sont entièrement fonctionnels et sont utilisés comme prévu avec le nombre maximal de personnes entrant et sortant via les points d'accès contrôlés et comme spécifié dans la documentation de conception.

Il convient que les alimentations avec raccordements au secteur utilisent un circuit électrique spécifique, protégé séparément.

Les exigences relatives à l'alimentation de secours de l'EACS installé et des composants des réseaux de communication qui lui sont associés doivent être prises en considération.

Les alimentations de secours doivent être capables d'alimenter les unités de contrôle d'accès et les accessoires, y compris les actionneurs fonctionnant dans des conditions de charge de fonctionnement spécifiées pendant la période de temps requise applicable à la classe de sécurité de l'EACS installé tel que cela est indiqué dans le Tableau 2.

Tableau 2 – Exigences sur l'alimentation pour un EACS installé

Exigences sur l'alimentation de secours	Attribution de classes			
	1	2	3	4
EACS devant continuer de fonctionner en cas de panne de la source primaire	OP	OP	M [a]	M [a]
Les sources d'alimentation de secours doivent être capables de fonctionner dans des conditions de charge spécifiées pendant la période de temps indiquée	OP	OP	2 h [b]	4 h

[a] Certains types d'actionneurs peuvent être exclus des exigences sur l'alimentation de secours dépendant de la classe (par exemple une alimentation en courant alternatif et/ou une forte consommation d'énergie) à condition que cela fasse l'objet d'un accord entre le propriétaire du système et l'installateur et que cela soit consigné dans la documentation du système conforme à l'exécution.

[b] Une période de secours plus courte peut être acceptable à condition qu'elle fasse l'objet d'un accord entre l'installateur et le propriétaire du système et qu'elle soit consignée dans la documentation du système conforme à l'exécution.

L'EACS peut avoir une ou plusieurs alimentations de secours. Le cas échéant, l'alimentation de secours d'un bâtiment peut être considérée comme une source d'alimentation de secours acceptable à condition qu'elle satisfasse aux exigences du Tableau 2.

Les conditions de charge de fonctionnement de l'alimentation de secours sont calculées en se basant sur les éléments suivants:

a) La consommation d'énergie nominale des équipements de l'EACS.
b) Le nombre prévu d'opérations (ouvertures et fermetures) par heure pour chaque point d'accès avec un actionneur à fermeture intégrée (c'est-à-dire un actionneur nécessitant de l'énergie pour ouvrir le point d'accès).
c) Le nombre maximal prévu d'actionneurs à fermeture intégrée alimentés simultanément et les exigences de charge de crête anticipées du système.
d) Chaque point d'accès équipé d'actionneurs à sécurité intrinsèque est alimenté en permanence (c'est-à-dire nécessitant de l'énergie pour garder le point d'accès fermé).

Un exemple de calculs de la capacité d'une batterie de secours est présenté à l'Annexe B.

Les EACS ne doivent pas empêcher la libre sortie autorisée par d'autres systèmes de secours (par exemple une alarme incendie).

8.2.2 Câblage

Il convient de sélectionner les chemins de câble de façon à assurer la distance la plus courte possible entre les emplacements des équipements. Des précautions doivent être prises pour s'assurer que les caractéristiques assignées d'incendie pour le bâtiment sont maintenues lorsque les câbles sont acheminés à travers les structures des bâtiments.

Il convient de prendre en considération la possibilité d'expansion future du système et de toute modification éventuelle du bâtiment/site.

Il convient de sélectionner les types de câble afin de réduire au minimum la chute de tension et la perte de signaux et de se conformer aux spécifications en matière d'environnement, de sécurité et de sûreté. Il convient que les valeurs des courants admissibles ne soient pas dépassées et que, dans la mesure du possible, des marges de sécurité adéquates soient prévues.

Il convient d'installer les câbles dans les zones de sécurité contrôlées et il convient qu'ils soient, dans la mesure du possible, cachés ou difficilement accessibles.

Il convient d'assurer une protection appropriée lorsque les câbles sont sujets à des risques de dommages matériels ou d'interférences délibérées. En cas de risque de dommages matériels, il convient de protéger mécaniquement le câble à l'aide, par exemple, de conduits, de gaines ou de tubes. Lorsque ces moyens de protection sont en matériau conducteur, il convient d'accorder une attention particulière à leur mise à la terre électrique appropriée et correcte.

Il convient de protéger physiquement les câbles reliant les parties de l'EACS contre les violations lorsqu'ils passent dans des zones ayant un niveau de sécurité inférieur.

Les conditions de circuit ouvert ou de court-circuit appliquées à des fils connectés à tout composant d'un système de contrôle d'accès installé à l'extérieur de sa zone de sécurité contrôlée ou accessible de l'extérieur de sa zone de sécurité contrôlée, ne doivent pas donner lieu à la mise en marche de l'actionneur de point d'accès permettant l'accès à la zone sécurisée. Lorsque le fonctionnement exige que le point d'accès soit sous le contrôle direct du système d'évacuation d'urgence (par exemple une alarme incendie), il convient que l'intégrité de l'interconnexion soit compatible avec le niveau de sécurité exigé par la classe de l'EACS.

L'alimentation électrique de chaque composant d'un EACS installé à l'extérieur de sa zone contrôlée doit être protégée contre les courts-circuits.

Il convient que les câbles très basse tension et de signalisation ne passent pas à proximité de l'alimentation secteur ou de câbles pouvant générer des interférences électriques.

9 Mise en service et mise à disposition du système

9.1 Mise en service

L'objectif du processus de mise en service est de confirmer que le système installé satisfait aux exigences de la conception du système.

Il convient que la procédure de mise en service fasse l'objet d'un accord écrit entre le propriétaire du système et les autres parties concernées.

Il convient de réaliser une inspection visuelle minutieuse pour s'assurer que l'installation, les méthodes, les matériaux et les composants utilisés soient conformes aux lignes directrices de la section 7.3 relatives à la conception du système et que la documentation du système conforme à l'exécution (y compris les dessins enregistrés, les consignes d'utilisation et les exceptions ayant fait l'objet d'un accord) corresponde à l'installation réelle.

A l'issue de la mise en service du système, et avant sa mise à disposition, il convient qu'une personne compétente inspecte et vérifie que le système fonctionne correctement et en particulier que:

a) les points d'accès fonctionnent;

b) les informations données par les composants de traitement sont correctes;

c) l'indication et l'annonce fonctionnent correctement;

d) les raccordements avec d'autres systèmes sont effectifs et les messages sont correctement compris par les autres systèmes;

e) les différents types d'annonce fonctionnent correctement;

f) les documents et les instructions pertinents ont été fournis;

g) le système continue à fonctionner en cas de mise hors tension du secteur (lorsque des sources d'alimentation de secours sont fournies).

Il n'est pas nécessaire que le processus de mise en service et de vérification comporte une entrée de données client réelle. Les essais peuvent être effectués avec des données temporaires.

9.2 Mise à disposition du système

La mise à disposition du système consiste à transférer formellement au propriétaire du système les responsabilités des sociétés de conception et d'installation. Il est recommandé que les conditions de mise à disposition du système soient clairement définies entre ces parties.

Il convient d'effectuer une démonstration complète de l'EACS et de prendre en compte les aspects suivants:

a) la documentation (voir l'Article 11);

b) la formation en gestion et en exploitation du système.

A l'issue de la mise à disposition du système, il convient de soumettre l'EACS à essai pendant une durée à convenir avec le propriétaire du système. Pendant cette période, il convient de faire fonctionner l'EACS normalement.

Il est également possible que la période d'essai s'inscrive dans le cadre du processus de mise en service et de vérification avant l'étape de la mise à disposition.

A la mise à disposition du système, il convient que le propriétaire du système soit informé des changements intervenus entre la conception du système et le système conforme à l'exécution et il convient qu'il soit invité à signer un certificat de réception indiquant que l'EACS a été installé et fonctionne conformément à la documentation du système conforme à l'exécution et que des instructions et des formations suffisantes ont été fournies pour assurer le bon fonctionnement de l'EACS.

10 Fonctionnement et maintenance du système

10.1 Fonctionnement du système

Il convient que le propriétaire du système s'assure que:

a) les utilisateurs et les opérateurs sont formés;

b) les instructions sont fournies aux utilisateurs et aux opérateurs;

c) les utilisateurs sont instruits et motivés sur la sécurité du site;

d) les procédures d'administration du système et de sauvegarde de données sont suivies;

e) les données du système sont mises à jour;

f) la réponse appropriée est apportée à toute alerte donnée;

g) les exigences réglementaires nationales en vigueur sont satisfaites;

h) des opérations régulières de maintenance du système sont organisées;

i) les mesures relatives à l'organisation sont en place en cas de panne de l'EACS.

Il convient que la société chargée de l'installation/maintenance informe le propriétaire du système de ses responsabilités en matière de gestion.

10.2 Maintenance du système

Pour s'assurer que l'EACS continue à fonctionner correctement, il convient de l'inspecter et de l'entretenir à intervalles convenus, par exemple deux fois par an, ou, si des diagnostics à distance sont possibles, l'inspection et l'entretien peuvent être réalisés une fois par an.

Il est recommandé de conclure des contrats de maintenance avant la mise en exploitation de l'EACS.

Il convient de signer un accord sur les niveaux de service de maintenance avec un organisme compétent pour l'inspection et l'entretien. Il convient que la maintenance ne soit assurée que par des personnes bien formées et compétentes dans les activités requises pour l'inspection et l'entretien du système.

Différents types de dispositions de maintenance peuvent être utilisés, par exemple:

a) des procédures d'inspection – action limitée à un contrôle diagnostique du système;
b) des procédures d'entretien – inspection suivie de la réparation ou du remplacement des pièces défaillantes du système.

Lors des travaux de maintenance, il peut être nécessaire de faire fonctionner l'EACS en mode dégradé.

Dans tous les cas, il convient que le personnel d'entretien informe l'opérateur du système et obtienne l'autorisation de procéder aux travaux de maintenance. Il est nécessaire de veiller à ce que, à la fin des travaux de maintenance, la pleine capacité de fonctionnement de l'EACS soit rétablie.

Il convient que la ou les procédures d'inspection et d'entretien soient fournies et documentées par le fabricant de composants ou l'installateur. Il convient que l'inspection et l'entretien soient effectués par l'organisme compétent suivant ces procédures et qu'ils comprennent l'inspection du fonctionnement des points d'accès.

En cas d'indication de dysfonctionnement (ou de dysfonctionnement futur éventuel) du système ou de dommages à une partie quelconque du système, il convient d'informer immédiatement l'organisme compétent pour assurer l'inspection et l'entretien.

Il convient que l'accord sur les niveaux de service de maintenance indique le type et la quantité de pièces de rechange à conserver et la possession de ces pièces afin que le niveau de fonctionnement convenu puisse être maintenu.

Il convient d'assurer des enregistrements du système pour consigner tous les dysfonctionnements du système, les actions de maintenance et les informations détaillées sur les modifications ou améliorations éventuelles apportées à l'EACS.

11 Documentation

11.1 Généralités

Il convient que la documentation nécessaire à l'installation, l'exploitation, la mise en service et la maintenance de l'EACS reflète la taille et la complexité du système installé et qu'elle soit fournie dans une langue convenue avec le propriétaire du système.

11.2 Documentation relative à la planification

Il convient que la documentation concernant l'installation proposée indique clairement:

a) la ou les zones de sécurité contrôlées;
b) l'emplacement du ou des équipements de reconnaissance;
c) la classification de chaque point d'accès;
d) l'emplacement de l'équipement de gestion;
e) les liaisons à établir entre les différents composants du système.

En fonction de la taille et de la complexité de l'installation, des informations spécifiques peuvent être nécessaires et peuvent couvrir:

1) les chemins de câble;
2) les détails d'interconnexion;
3) les schémas du système;
4) les ouvrages de référence du produit.

11.3 Documentation relative à la mise en service/mise à disposition du système

Il convient de produire la documentation du système conforme à l'exécution sur la base du projet de conception du système et de l'amender afin d'inclure les modifications apportées à la conception de l'EACS jugées nécessaires au cours du processus d'installation afin qu'elle décrive l'état exact de l'EACS installé.

Il convient que la documentation du système conforme à l'exécution comprenne des informations portant sur:

a) la description du système installé;
b) l'emplacement des composants du système;
c) les chemins de câble pertinents;
d) les plans d'interconnexion détaillés;
e) les paramètres de configuration.

Il convient de fournir les documents suivants au propriétaire du système. Il convient que le propriétaire du système mette ces documents à disposition en cas de nécessité de procéder à la modification, la réparation ou la maintenance de l'EACS. Il convient également qu'il s'assure que les documents sont tenus à jour:

1) la documentation du système conforme à l'exécution;
2) les consignes d'utilisation du système;
3) les manuels du système et des composants;
4) les coordonnées de l'installateur/fournisseur de service

11.4 Documentation relative à la maintenance

Il convient que la documentation comporte des instructions pour la maintenance préventive, les intervalles de remplacement de la batterie de secours et le programme d'inspection du système installé.

Annexe A
(normative)

Exceptions autorisées pour les systèmes installés

A.1 Généralités

La présente norme indique que l'EACS installé doit satisfaire aux exigences données d'une classe dans l'IEC 60839-11-1, mais le 7.3.1 autorise des exceptions spécifiques aux applications pour ces exigences.

Les exigences données dans l'IEC 60839-11-1 sont principalement destinées aux EACS fabriqués et ne correspondent donc pas exactement aux exigences attendues pour des EACS installés.

L'Annexe A donne des informations sur les exceptions autorisées par rapport aux exigences données d'une classe dans l'IEC 60839-11-1 considérées comme les mieux adaptées aux cas pratiques.

Les installateurs, les clients, les rédacteurs de descriptifs et les utilisateurs finaux peuvent se référer à cette annexe pour réduire le besoin d'expliquer et de documenter les raisons des exceptions.

Toutes les exceptions doivent faire l'objet d'un accord entre l'installateur et l'utilisateur final et être consignées dans la documentation du système conforme à l'exécution. Il convient que l'installateur indique la façon dont ces exceptions peuvent affecter les fonctions et la sécurité de l'EACS.

A.2 Déclarations de conformité

Les déclarations de conformité conformes à l'IEC 60839-11-2 doivent inclure une référence aux exceptions mises en œuvre autorisées à l'Annexe A.

A.3 Exceptions autorisées

Si une fonction est prévue, elle doit satisfaire aux exigences applicables de la classe pour laquelle la conformité est déclarée.

Les Tableaux A.1 à A.8 suivants donnent une liste des exceptions autorisées (indiquées en ***gras italique***) applicables uniquement à un EACS installé.

NOTE Les numéros des lignes des tableaux correspondent aux numéros des lignes des tableaux respectifs de l'IEC 60839-11-1

Tableau A.1 – Exceptions autorisées pour les exigences concernant les interfaces de points d'accès

Exigences concernant les interfaces de points d'accès (IEC 60839-11-1:2013, 6.2, Tableau 2)		Attribution de classes			
		1	2	3	4
6	Prévoir un contrôle d'accès pour la sortie d'une zone protégée (contrôlée)	OP	***OP***	***OP***	M
7	Anti retour rigide	OP	OP	***OP***	M
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	***OP***

Tableau A.2 – Exceptions autorisées pour les exigences concernant l'indication et l'annonce

Exigences concernant l'indication et l'annonce (IEC 60839-11-1:2013, 6.3, Tableau 3)					Attribution de classes			
					1	2	3	4
A – Accès contrôlé (indication locale)								
		Indication						
4	L'indication visuelle et/ou sonore est requise pour la dernière période (temps de préalerte) 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	***OP***	***OP***
B – Console de commande (annonciation)								
		Affichage	Alerte	Enregistrement				
6	Un enregistrement est requis lorsque l'accès est autorisé			•	OP	OP	***OP***	M
7	L'annonce visuelle, l'alerte et l'enregistrement sont requis pour les conditions d'agression. Le signalement d'agression n'est pas obligatoire. Lorsqu'un signalement d'agression est prévu, une annonce visuelle, une alerte et un enregistrement sont requis pour les conditions d'agression.	•	•	•	OP	OP	OP	***OP***
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	***OP***	M
17	Accès refusé. Peut être configurable par accès contrôlé conformément à l'exigence de classe. Il est obligatoire que les installations d'EACS de classes 3 et 4 aient activé l'affichage, l'alerte et l'enregistrement des événements d'accès refusé.	•	•	•	OP	OP	M	M
25	Appel nominal	•		•	OP	OP	***OP***	***OP***
35	Etat du lecteur hors tension	•	•	•	OP	OP	OP	***OP***
37	Annonce d'atteinte d'une limite de 90 % par rapport à la capacité maximale	•	•	•	OP	OP	M	M

Exigences concernant l'indication et l'annonce (IEC 60839-11-1:2013, 6.3, Tableau 3)					Attribution de classes			
					1	2	3	4
	d'enregistrement. Il est recommandé que les installateurs de réfèrent aux informations du fabricant et qu'ils indiquent à l'utilisateur final l'importance et les conditions d'apparition de cet événement.							
41	Le système doit être capable d'attribuer des niveaux de priorité aux événements d'alerte spécifiques	•			OP	OP	***OP***	***OP***

Tableau A.3 – Exceptions autorisées pour les exigences concernant la reconnaissance

Exigences concernant la reconnaissance (IEC 60839-11-1:2013, 6,4, Tableau 4)		Attribution de classes			
		1	2	3	4
	A – Niveaux d'accès				
6	Nombre minimum de niveaux d'accès utilisateur NOTE Le nombre minimum n'est pas défini.	***OP***	***OP***	***OP***	***OP***
7	Nombre minimum de périodes configurables NOTE Le nombre minimum n'est pas défini.	***OP***	***OP***	***OP***	***OP***
9	La résolution temporelle minimale d'un niveau d'accès inclut le jour du mois, le mois et l'année	N/A	OP	OP	***OP***
24	Prise en charge de plusieurs codes d'installation si le système utilise le codage d'installation	OP	OP	OP	***OP***

Tableau A.4 – Exigences concernant le signalement d'agression

Exigences concernant le signalement d'agression (IEC 60839-11-1:2013, 6,5, Tableau 5)	Attribution de classes			
	1	2	3	4
Le signalement d'agression n'est pas obligatoire. Lorsque le signalement d'agression est mis en œuvre, il doit satisfaire aux exigences de l'IEC 60839-11-1:2013, Tableau 5.				

Tableau A.5 – Exigences concernant la neutralisation

Exigences concernant la neutralisation (IEC 60839-11-1:2013, 6.6, Tableau 6)	Attribution de classes			
	1	2	3	4
Aucune exception n'est autorisée.				

Tableau A.6 – Exigences concernant la communication

Exigences concernant la communication (IEC 60839-11-1:2013, 6.7)	Attribution de classes			
	1	2	3	4
Aucune exception n'est autorisée.				

Tableau A.7 – Exceptions autorisées pour les exigences concernant l'autoprotection des systèmes

Exigences concernant l'autoprotection des systèmes (IEC 60839-11-1:2013, 6.8, Tableau 7)		Attribution de classes			
		1	2	3	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). Cette exigence s'applique à l'accès au système dans le cadre de la configuration. L'exigence ne génère donc pas de conflit avec les exigences concernant la reconnaissance de l'IEC 60839-11-1:2013, Tableau 4.	4N	5N	6A	8A
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). Exception: il convient que le système n'empêche pas les individus de modifier leurs propres informations mémorisées.	OP	OP	M	M
15	L'identifiant d'accès logique peut être attribué uniquement par l'administrateur système. Exception: il convient que le système n'empêche pas les individus de modifier leurs propres informations mémorisées.	OP	OP	M	M
18	Cryptage requis pour les signaux de communication entre les composants de l'EACS lors de l'utilisation de réseaux partagés en commun (par exemple l'Internet). NOTE L'utilisation d'un réseau privé virtuel n'est pas considérée comme un réseau partagé en commun.	OP	OP	M	M
19	Les informations mémorisées sur le jeton doivent être protégées contre toute modification ou reproduction non autorisée. (Pour la classe 3 uniquement): lorsque l'exigence ci-dessus ne peut pas être satisfaite, il convient de considérer l'utilisation d'une combinaison de deux méthodes de reconnaissance ou plus.	OP	OP	M	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. Pour la classe 4, il est obligatoire de se conformer à l'élément 24. Pour la classe 3, les fabricants doivent obligatoirement se conformer à l'élément 24 ou à l'élément 25 (ou aux deux). Il convient que les installateurs respectent les exigences d'installation indiquées par les fabricants si la conformité est obtenue par l'élément 25.	OP	OP	OP*	OP

Tableau A.8 – Exceptions autorisées pour les exigences concernant l'alimentation

Exigences concernant l'alimentation (IEC 60839-11-1:2013, 6.9, Tableau 8)	Attribution de classes			
	1	2	3	4
Les exceptions autorisées sont données au 8.2.1, Tableau 2.				

Annexe B
(informative)

Calculs de la capacité d'une batterie de secours

La capacité minimale d'une batterie de secours peut être calculée comme suit:

Mesure	Unité	Description	Exemple
n_i	Par heure	Nombre prévu d'activations par heure (ouverture et fermeture d'un accès contrôlé) par accès contrôlé	150, 30, ...
t_{acti}	Secondes	Durée d'une activation pour un actionneur à fermeture intégrée	2, 5, ...
I_{equip}	Ampères	Consommation d'énergie des équipements d'un EACS (sans les actionneurs)	0,5
$I_{fail\text{-}secure}$	Ampères	Consommation d'énergie de tous les actionneurs à fermeture intégrée (à l'état activé)	2
$I_{fail\text{-}safe}$	Ampères	Consommation d'énergie de tous les actionneurs à sécurité intrinsèque (à l'état activé)	3
t	Heures	Période de secours exigée	2
D_i	%	Cycle de fonctionnement (pourcentage de temps d'activations par heure) par accès contrôlé	
I_{avg}	Ampères	Charge moyenne pour les conditions de charge prévues	
C	Ah	Capacité minimale exigée pour la batterie	

$D_i = t_{acti} \times n_i / 3\,600$	Exemple: $D_1 = 2 \times 150/3\,600$ $D_1 = 8{,}33$ % $D_2 = 5 \times 30/3\,600$ $D_2 = 4{,}17$ %

$I_{fail\text{-}safe} = I_{fail\text{-}safe1} + I_{fail\text{-}safe2} + \ldots$ $I_{fail\text{-}secure} = I_{fail\text{-}secure1} \times D_1 + I_{fail\text{-}secure2} \times D_2 + \ldots$	Exemple: $I_{fail\text{-}safe} = 0{,}5 + 0{,}3 + \ldots = 3$ A $I_{fail\text{-}secure} = 0{,}4 \times 0{,}083\,3 + 0{,}6 \times 0{,}041\,7 + \ldots = 0{,}17$ A

$I_{avg} = I_{equip} + I_{fail\text{-}secure} + I_{fail\text{-}safe}$	Exemple: $I_{avg} = 0,5 + 0,17 + 3$ $I_{avg} = 3,67$ A

$C = t \times I_{avg}$	Exemple: $C = 2 \times 3,67$ $C = 7,34$ Ah

Choix de batterie NOTE Le choix tient compte du facteur de déclassement dérivé des spécifications du fabricant.	On suppose un facteur de déclassement de 20 % $C = 7,34 \times 1,2$ $C = 8,8$ Ah On choisit donc une batterie de capacité minimale supérieure à 8,8 Ah (dans ce cas, une valeur normalisée de capacité de batterie peut être 10 Ah).

Pour choisir la capacité de la batterie, il est recommandé d'introduire un facteur de déclassement tenant compte des spécifications du fabricant de batteries (par exemple le type de batterie, les effets du vieillissement, la température de fonctionnement, etc.).

Bibliographie

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

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

IEC 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*

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

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

_____

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