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 It also gives information on projects, replaced and withdrawn publications.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

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-2: 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

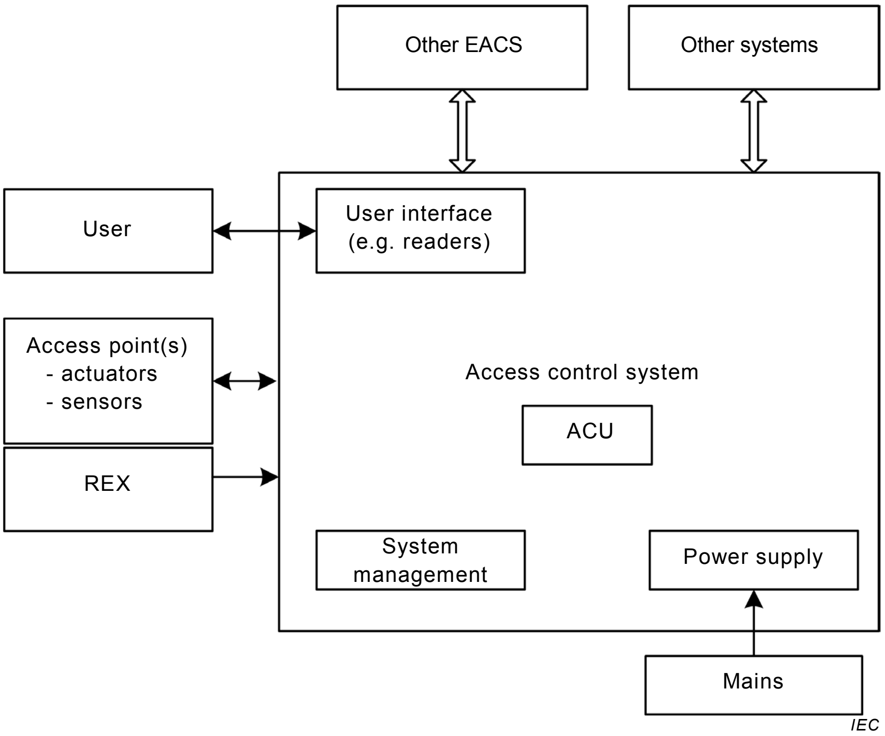
For the purposes of this document, the abbreviations given in IEC 60839-11-1, as well as the following apply.

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.

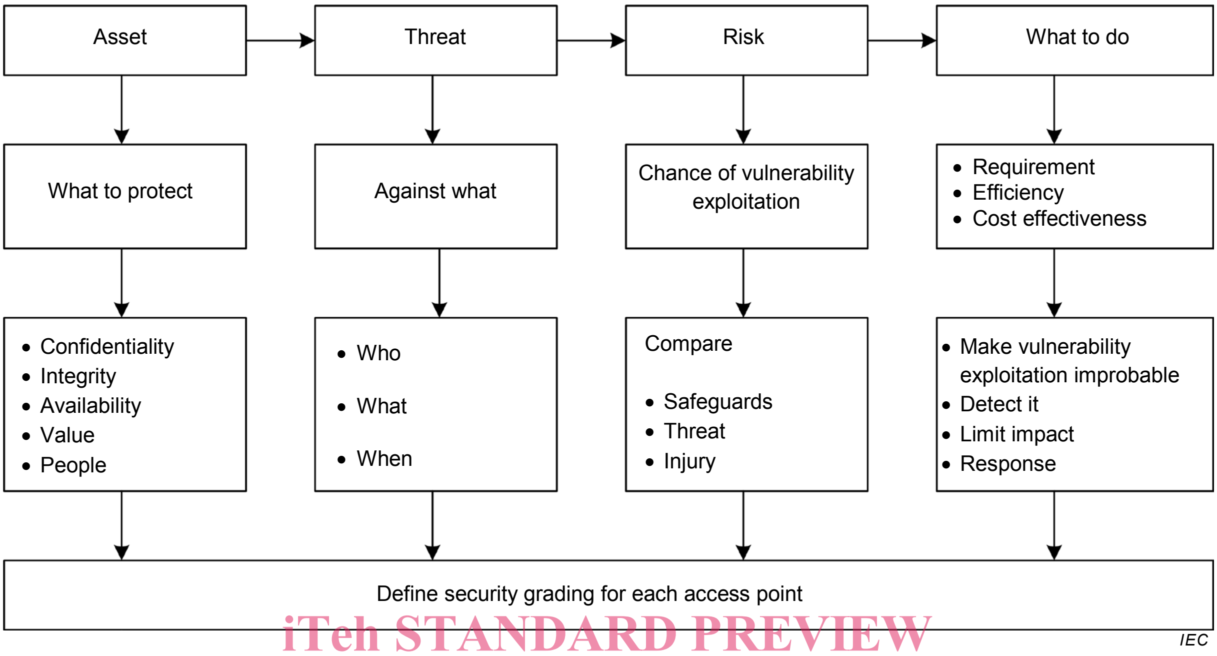


Figure 2 – Risk assessment chart

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).

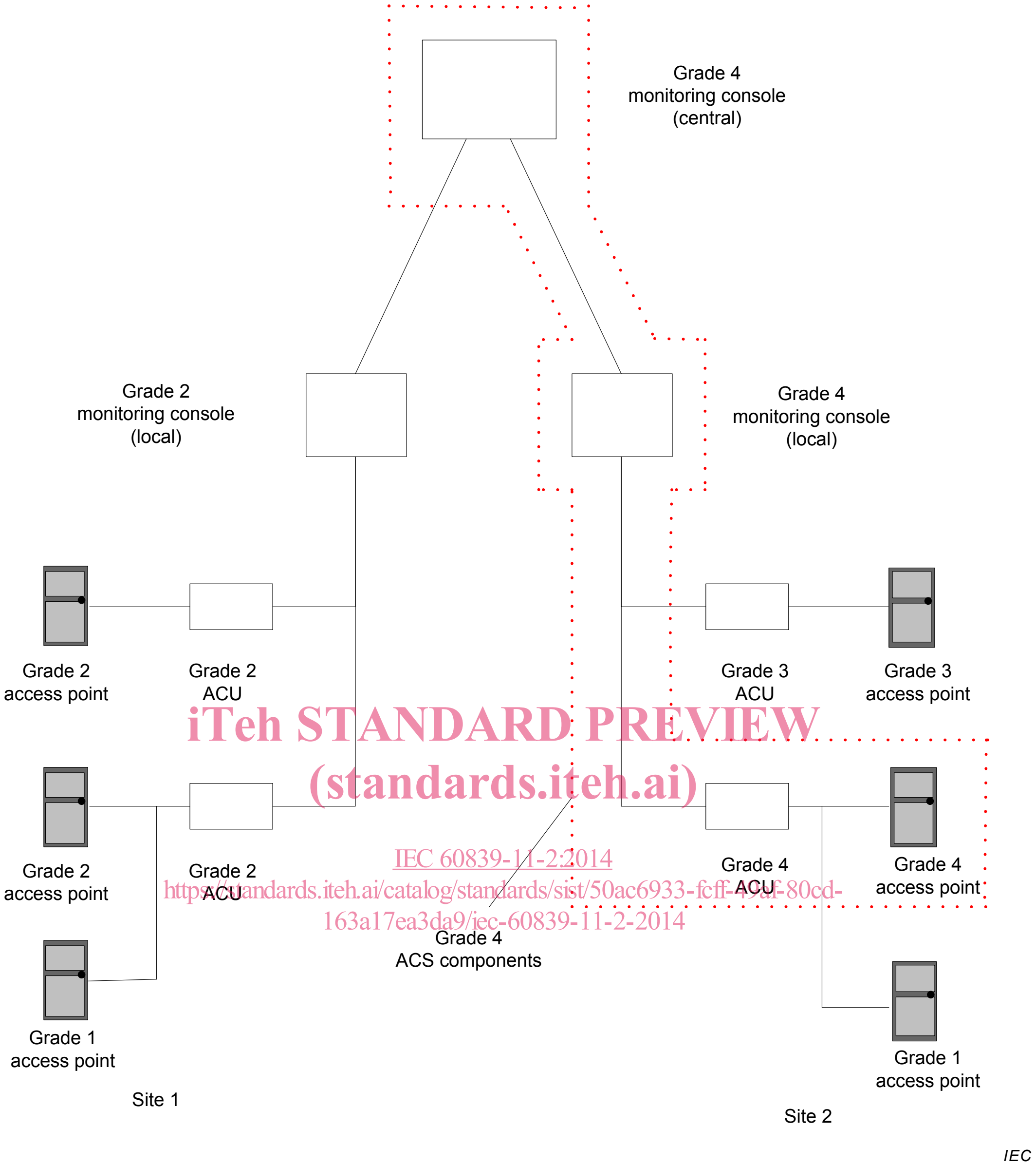


Figure 3 – Example of system grade selection

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.