IEC 62642-3

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems – Intrusion and hold-up systems – Part 3: Control and indicating equipment

Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 3: Equipement de contrôle et de signalisation

IEC 62642-3:2010

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62642-3

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems – Intrusion and hold-up systems – Part 3: Control and indicating equipment

Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 3: Equipement de contrôle et de signalisation

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE CODE PRIX XC

ICS 13.320

ISBN 978-2-88912-198-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM SYSTEMS – INTRUSION AND HOLD-UP SYSTEMS –

Part 3: Control and indicating equipment

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 62642-3 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

This standard is based on EN 50131-3 (2006).

The text of this standard is based on the following documents:

FDIS	Report on voting
79/310/FDIS	79/321/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 of the IEC 62642 series can be found, under the general title *Alarm systems – Intrusion and hold-up systems*, on the IEC website.

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.

INTRODUCTION

This part 3 of the IEC 62642 series of standards gives requirements for control and indicating equipment used in intrusion and hold-up alarm systems. The other parts of this series of standards are as follows:

Part 1 System requirements
Part 2-2 Intrusion detectors – Passive infrared detectors
Part 2-3 Intrusion detectors – Microwave detectors
Part 2-4 Intrusion detectors – Combined passive infrared / microwave detectors
Part 2-5 Intrusion detectors – Combined passive infrared / ultrasonic detectors
Part 2-6 Intrusion detectors – Opening contacts (magnetic)
Part 2-71 Intrusion detectors – Glass break detectors – Acoustic
Part 2-72 Intrusion detectors – Glass break detectors – Passive
Part 2-73 Intrusion detectors – Glass break detectors – Active
Part 3 Control and indicating equipment
Part 4 Warning devices
Part 5-3 Interconnections – Requirements for equipment using radio frequency techniques
Part 6 Power supplies
Part 7 Application guidelines
Part 8 Security fog devices/systems

In order to insure the consistency of the whole IEC 62642 series, the terminology is defined at one place that is the master document IEC 62642-1 that gives general requirements concerning the intrusion system. Exception is made for specific terms to control and indicating equipment and where repetition is deemed essential for the clarity of this document.

Reference has been included to various implications arising from the detector standards. Full detail of the interconnection requirements could be the subject of a future standard.

A number of requirements are contained in this standard for which a formal test procedure can only be written by defining (and hence restricting) the technology by which the requirement is achieved. Accordingly, it has been recognised that such functions can be tested only by agreement between manufacturer and test house, according to documented information relating to how the required functionality has been achieved.

A table to cross reference IEC 62642-1 requirements against this standard and tests has been included in Annex D.

ALARM SYSTEMS – INTRUSION AND HOLD-UP SYSTEMS –

Part 3: Control and indicating equipment

1 Scope

This part of the IEC 62642 specifies the requirements, performance criteria and testing procedures for control and indicating equipment (CIE) intended for use in intrusion and hold-up alarm systems (I&HAS) installed in buildings. This document also applies to CIE to be used in IAS or HAS.

The CIE may incorporate processing functions of other I&HAS components or its processing requirements may be distributed among such components.

This standard specifies the requirements for CIE installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to ancillary control equipment (ACE) that are installed inside or outside of the supervised premises and mounted in indoor or outdoor environments.

Where CIE shares means of detection, interconnection, control, communication, processing and/or power supplies with other applications, these requirements apply to I&HAS functions only.

This standard specifies performance requirements for CIE at each of the four security grades identified in the IEC 62642-1. Requirements are also specified for four environmental classes covering applications for indoor and outdoor locations.

This standard includes mandatory functions, which shall be provided on all CIE for the appropriate security grade, as well as optional functions that may additionally be provided.

NOTE In this standard reference to the term “I&HAS” is used throughout, except where there is specific need to differentiate between the IAS and HAS portions of a system. The term is intended to include IAS and HAS when such systems are installed separately.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60068-1:1988, *Environmental testing – Part 1: General and guidance*

IEC 60068-2-75:1997, *Environmental testing – Part 2-75: Tests – Test Eh: Hammer tests*

IEC 60073, *Basic and safety principles for man-machine interface, marking and identification – Coding principles for indicators and actuators*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 62599-1, *Alarm systems – Part 1: Environmental test methods*

IEC 62599-2, *Alarm systems – Part 2: Electromagnetic compatibility – Immunity requirements for components of fire and security alarm systems*

IEC 62642-1:2010, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

IEC 62642-5-3, *Alarm systems – Intrusion and hold-up systems – Part 5-3: Interconnections – Requirements for equipment using radio frequency techniques*

EN 50131-6:2008, *Alarm systems – Intrusion and hold-up systems – Part 6: Power supplies*[1]

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the IEC 62642-1, as well as the following, apply.

3.1.1
acknowledge
action of a user to accept an indication

3.1.2
alarm point
one or more detector(s) providing a common signal or message, at the CIE or at the ACE for the purpose of indication or processing

3.1.3
alarm signal or message
signal or message generated by an alarm point

3.1.4
biometric key
use of biometric characteristic by an authorized user to gain access to restricted functions or parts of a CIE

EXAMPLE: finger print or iris recognition.

3.1.5
conditioning
exposure of the Equipment Under Test (EUT) to environmental conditions in order to determine the effect of such conditions on the EUT

3.1.6
detector
device designed to generate an alarm signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard

3.1.7
digital key
portable device containing digitally coded information used by an authorized user to gain access to restricted functions or parts of a CIE

EXAMPLE: magnetic card, electronic token or similar.

---

1 The transformation of this document as IEC 62642-6 is under preparation.

3.1.8
entry route facility
means to ignore signals or messages from specified detectors during unsetting for a specified time period

3.1.9
entry time
time permitted for unsetting procedure where entry route is used

3.1.10
exit route facility
means to ignore signals or messages from specified detectors during setting for a specified period

3.1.11
external power source
EPS
energy supply external to the I&HAS which may be non-continuous

EXAMPLE: main power supply.

NOTE For Type A and Type B PS only. The EPS is derived as described in EN 50131-6.

3.1.12
fail to set

condition when defined setting procedure has not been completed within a specific time so that I&HAS is left in the “setting mode”

3.1.13
false acceptance rate
FAR

proportion of biometric verification transactions with wrongful claims of identity that are incorrectly accepted

3.1.14

false rejection rate
FRR
proportion of biometric verification transactions with truthful claims of identity that are incorrectly denied

3.1.15
interaction
any deliberate operation or act by the user to control or vary the function of the I&HAS

3.1.16
intrusion
entry into the supervised premises by an unauthorised person(s)

3.1.17
logical key
logical information used by an authorized user to gain access to restricted functions or parts of a CIE

EXAMPLE: PIN code, digital key, biometric key.

3.1.18
mechanical key
implement relying solely on physical shape to determine its uniqueness, used by an authorized user to gain access to restricted functions or parts of a CIE

3.1.19
non-I&HAS interface
device external to the I&HAS used to carry out some or all ACE functions

EXAMPLES: Computer, PDA.

3.1.20
operating mode
set, unset, setting and unsetting are the four operating modes

3.1.21
open by normal means
opening of the equipment housing by the procedure defined by the manufacturer

3.1.22
personal identification number
PIN code
code used by an authorised user to gain access to restricted functions or parts of a CIE (example, numeric or alphanumeric)

3.1.23
soak
an attribute of an alarm point such that signals or messages that normally create notifications are prevented from doing so, but continue to be recorded in the event log

3.1.24
storage device
SD
device which stores energy

EXAMPLE: a battery.

3.1.25
supervised premises transceiver
SPT
equipment at the supervised premises, including the interface to the I&HAS and the interface to the alarm transmission network.

3.1.26
test condition
condition of an alarm system in which the normal functions are modified for test purposes

3.1.27
user input
command generated by a deliberate user action

3.1.28
user input device
device used for user input

EXAMPLES: ACE, physical lock with electrical contacts.

3.2 Abbreviations

For the purposes of this document, the following abbreviations are used.

ACE ancillary control equipment
APS alternative power source
ARC alarm receiving centre
CIE control and indicating equipment
EPS external power source
EUT equipment under test
FAR false acceptance rate
FRR false rejection rate
HAS hold-up alarm system
IAS intrusion alarm system
I&HAS intrusion and hold-up alarm system
PDA personal digital assistant
PIN personal identification number
PS power supply
SD storage device
SPT supervised premises transceiver
WD warning device

4 Equipment attributes

4.1 General

CIE shall include attributes for the reception of signals and/or messages, processing the information, notification and indication as appropriate. The detailed requirements are provided in Clause 8.

NOTE If a function is provided that is optional for a particular grade and a claim of compliance is made, it should meet the applicable requirements for the grade for which compliance is claimed (if any are given). If there are no specifications for the function at the grade in question, the requirements for any higher grade (as identified by the manufacturer) apply.

Compliance with this standard shall be demonstrated by assessment of Clause 4 through to Clause 10 and the application of the tests of Clause 11.

Annex D provides a cross reference between the requirements of IEC 62642-1 and the requirements and tests of this standard.

4.2 Functionality

Functions additional to the mandatory functions specified in this standard may be included in I&HAS providing they do not influence the correct operation of the mandatory functions.

Where provided, these additional functions shall not affect compliance with the requirements of this standard, except as permitted by IEC 62642-1, 8.3.13.

It is permitted for the CIE to include functionality for special purposes that would render the I&HAS non-compliant with IEC 62642-1. The manufacturer's documentation shall include a warning to this effect.

If use of a function(s) or combination of functions within the CIE would result in the installed I&HAS not being compliant with IEC 62642-1 or being compliant at a lower security grade (examples are function(s) reducing the security of the I&HAS) the manufacturer shall, either:

a) detail the configuration(s) which are compliant with IEC 62642-1;

or

b) detail the function(s) or combination of functions that would result in the installed I&HAS not being compliant with IEC 62642-1.

The manufacturer shall document the fact that compliance labelling should be removed or adjusted if non-compliant configurations are selected.

5 CIE construction

The CIE may be in a single housing or be distributed in multiple housings and may be combined with other I&HAS components.

Provision shall be made to allow adequate fixing of the housing to the mounting surface.

Use of equipment not part of the I&HAS may be used to carry out ACE functions (examples are computer, PDA) if the conditions specified in Annex C are met.

6 Security grade

The CIE and ACE shall be declared to comply with one of four security grades (with grade 1 being the lowest and grade 4 being the highest) and shall meet all the requirements of that grade.

The requirements for the performance of the CIE will vary depending upon its grade. Any testing will be carried out according to the grade declared in the CIE documentation and marking.

7 Environmental performance

7.1 Requirements

CIE and ACE shall be suitable for use in at least one of the environmental classes defined in IEC 62642-1.

When the requirements of the four environmental classes are inadequate, due to the extreme conditions experienced in certain geographic locations, special national conditions are given in IEC 62642-1, Annex A.

7.2 Environmental and EMC tests

IEC 62599-2 specifies EMC susceptibility tests relevant to I&HAS components. The operating conditions for these tests are specified in Table 32 of this standard.

IEC 62599-1 describes environmental test methods relevant to I&HAS components. The tests applicable are specified in Table 32 of this standard.

NOTE Other environmental aspects, covered by Regional Regulatory Directives, are outside the scope of this standard.

8 Functional requirements

8.1 Inputs

Depending on the grade of the CIE and ACE, means shall be provided to receive signals or messages from detectors, hold-up trigger devices and information from user input devices as specified in the following subclauses.

NOTE 1 This standard does not specify details of interconnections or the format of these signals or messages. Details of possible means of transfer of the information are included in some of the component standards belonging tothe IEC 62642 series.

NOTE 2 Some system components may require up to 180 s to initialise before normal functionality is available (for example: detectors).

8.1.1 Intruder detection

The CIE shall provide the means to receive signals or messages from intruder detectors.

8.1.2 Hold-up device

When a CIE provides hold-up facilities, means shall be provided to receive signals or messages from hold-up devices.

8.1.3 Tamper

The CIE shall provide the means to receive tamper signals or messages.

8.1.4 Fault

Dependent on the grade, CIE shall include means to recognize the fault conditions as specified in Table 1 of IEC 62642-1, and in addition those faults shown in the Table 1 below.

Table 1 – Recognition of additional fault conditions

Faults	Grade 1	Grade 2	Grade 3	Grade 4
Battery change required [a]	M	M	M	M
Power output fault [b]	Op	Op	M	M
Monitoring of processing	Op	Op	M	M
M = Mandatory Op = Optional [a] applies to type “C” PS only as defined in EN 50131-6. [b] as in EN 50131-6, 4.2.5.				

8.1.5 User input

The CIE shall provide the means to receive information from user input devices (for example: a keypad or switch).

8.1.6 Masking

The CIE shall provide the means to receive masking signals or messages, according to grade.

The CIE shall process masking signals or messages when the system is set and optionally when unset.

8.1.7 Movement detector range reduction

The CIE shall provide the means used to receive reduction of range signals or messages, according to grade.

NOTE The means to convey movement detector reduction of range signals or messages from detectors may not permit differentiation from masking events. See detector standards.

8.1.8 Non-I&HAS inputs

When a CIE receives signals or messages or other information not necessary to meet the requirements of this standard (for example: monitoring of non-I&HAS equipment), this shall not affect the ability of the CIE to meet the requirements of this standard.

8.2 Outputs

Notification output requirements are detailed in 8.6

The CIE may need to provide output signals or messages to interface with other I&HAS components, as required by other relevant component standards. The installation documentation shall identify which configurations are available.

EXAMPLES:

a) indication enable for detector or other component;

b) set/unset status information for detector, security fog device, etc.;

c) to trigger audible or visual alarm confirmation equipment;

d) to trigger security fog devices, etc.;

e) to enable functional test mode of detector;

f) to trigger remote self-test of detector or other component;

g) to restore detectors or other devices.

NOTE If the restore involves removal of power from detectors, up to 180 s should be allowed for the detector to resume normal operation (see IEC 62642-2 series).

Output signals or messages may additionally be provided to interface to equipment outside of the I&HAS (for example: lighting).

8.3 Operation

The CIE shall provide the means necessary to enable authorized users to access the functions of the CIE. Access to these functions shall be restricted by access levels and corresponding authorisations according to 8.3.1 and 8.3.2 (for example by using a keypad or lock).

8.3.1 Access levels

Access to the functions of a CIE shall be restricted according to the requirements of IEC 62642-1, 8.3.1. If the CIE includes security functions additional to those identified in the Table 2 of the IEC 62642-1, the access levels necessary to operate those functions shall be specified by the manufacturer. Access levels for any non-security functions shall be specified in the manufacturer's documentation.

Access at level 3 shall be authorized by access level 2 such that:

a) access remains authorized until manually removed,

or

b) access requires authorization for each occasion it is used.

Access at level 4 shall be authorized by access level 2 and 3 for each occasion it is used.

If level 3 access is granted without level 2 authorisation, as permitted by IEC 62642-1, 8.3.1, the internal warning device shall be time limited, either to a fixed time quoted by the manufacturer or until silenced by the level 3 user.

8.3.2 Authorization

Access to the functions of a CIE (as defined) at levels 2, 3 and 4 shall be restricted as required by IEC 62642-1, 8.3.2. Authorization is not required for access at level 1.

Authorization shall be validated by the CIE.

NOTE If means to provide temporary authorization is provided (for example PIN code valid for a limited time or valid for use a specified number of times), details should be included in the manufacturer's documentation.

8.3.2.1 Use of mechanical key

Where mechanical keys are used, the manufacturer shall supply sufficient information to establish the number of combinations available.

8.3.2.2 Use of logical keys

Where logical keys are used, the manufacturer shall supply sufficient information to establish the number of combinations available.

Additionally the following apply to specific types of logical key. This does NOT restrict use of other types.

8.3.2.2.1 Use of PIN codes

Where PIN codes are used, the number of combinations not available shall be identified by the manufacturer and shall be disallowed from calculation of codes available.

Means shall be provided to prevent reading of authorization codes.

Entry of a code shall be completed within 60 s. If the code entry is not completed in that time, it shall be treated as invalid in the context of 8.3.2.4.

8.3.2.2.2 Digital keys

Where a user can complete the setting or unsetting procedure from a location more than 1 m from the CIE or ACE, digital keys used for I&HAS of grades 3 and 4 shall include means to prevent acceptance of keys copied from intercepted data (for example: rolling codes).

Where the operation can be performed other than at the point of exit from the premises, means shall be provided to make the “prevention of setting” and “completion of setting” indications available to the user (for example: on the key).

Self-powered digital keys shall monitor storage device charge as required by EN 50131-6, 4.2.2 and report battery low condition to the CIE (via ACE where applicable) each time the device is used for setting or unsetting. This report shall be made on each event for a minimum of 25 such events, over a period not exceeding 1 month and shall result in an indication and event log entry (including the identity of the relevant user) each time the condition is reported.

When a low battery condition is identified at the time of setting, the I&HAS shall not set until the low battery indication has been manually acknowledged at the CIE or ACE. This acknowledgement shall be logged at grade 2 and above.

8.3.2.2.3 Biometric keys

Where biometric means are used for authorization, the recognition coding structure shall provide a minimum number of combinations as shown in Table 2. Each recognition information presented to the system shall be compared with this structure. The false acceptance and false rejection rates shall not exceed the values shown in Table 2.

Table 2 – Recognition of biometric keys

	Grade 1	Grade 2	Grade 3	Grade 4
Number of combinations	1 000	10 000	100 000	1 000 000
False acceptance rate (FAR)	< 0,1 %	< 0,1 %	< 0,01 %	< 0,001 %
False rejection rate (FRR)	< 1 %	< 1 %	< 1 %	< 1 %

If the FAR and FRR are adjustable, the means of adjustment shall permit identification of the parameters to ensure compliance with the above grades. This information shall be included in the manufacturer’s documentation.

NOTE Additional characteristics of specific types of biometric device should be considered according to the suitability for the assessed risk of the I&HAS (for example: ease with which the biometric characteristic may be compromised).

8.3.2.3 Use of methods of authorization in combination

Two or more devices or technologies may be used by one or more individuals to authorize level 2 or level 3 access to a CIE (for example: use of PIN code plus digital key).

The combination of operations shall be validated by the CIE.

The maximum time between completion of one operation and initiation of the next shall be restricted by grade according to Table 3:

Table 3 – Time intervals for methods of authorization used in combination

	Grade 1	Grade 2	Grade 3	Grade 4
Time permitted	1 min	1 min	30 s	15 s

The number of combinations for each device is multiplied to assess the resulting grade compliance.

NOTE 1 Two different technologies may be used by same person.

NOTE 2 Two devices of same technology may be allocated to different people.

NOTE 3 Two technologies may be combined into a single device (for example: mechanical key with integrated digital key).

8.3.2.4 Detection of repeated invalid authorization attempts

Depending on the grade, when a CIE uses logical keys to restrict access or when the CIE has the means to identify individual mechanical keys, means shall be provided to detect and record repeated attempts to gain access not recognised as valid by the CIE, as specified in Table 4.

When required by Table 4, the user input device(s) at which the invalid attempts are made shall be disabled for a minimum of 90 s. Other or all user input devices may also be disabled.

Tamper shall not be activated when less than 3 invalid attempts are detected.

The CIE may treat repeated use of the same invalid logical key as a single attempt.

Table 4 – Detection of repeated invalid authorization attempts

	Grade 1	Grade 2	Grade 3	Grade 4
Disable user input device(s)	Op	Op [a]	M	M
Maximum number of attempts before user input device(s) initially disabled	10	10	10	3
Maximum number of further attempts before user input device(s) disabled	10	10	1	1
Record in event log each time user input device(s) disabled	Op	Op	Op	M
Tamper signal or message	Op	Op [a]	Op	M
Maximum number of attempts before tamper activated	21	21	21	7

M = Mandatory
Op = Optional

[a] For grade 2 at least one of these requirements shall be provided.

8.3.3 Setting procedures

CIE shall provide means for a user to set the I&HAS or part thereof in accordance with IEC 62642-1, 8.3.3 and 8.3.4.

NOTE 1 It is not mandatory to provide means to set a HAS or the HAS portion of an I&HAS.

The CIE may provide means to set automatically at pre-determined times (time dependent). When means are provided to set at pre-determined periods, the CIE shall generate at least one indication before commencing setting. Details of the pre-setting indication(s) shall be included in manufacturer's documentation.

NOTE 2 This indication should enable a user on the premises to be aware of the imminent setting of the I&HAS.

If setting at grade 1 is implemented as permitted by IEC 62642-1, 8.3.4, means shall be provided to cancel the setting procedure before it is completed. This shall not permit cancelling the setting procedure if started by other means.

8.3.3.1 Prevention of setting and overriding of prevention of setting

The CIE shall provide means to prevent the setting of the system in accordance with IEC 62642-1, 8.3.5 and may provide means to override such prevention of setting in accordance with IEC 62642-1, 8.3.6.

Where the prevention of setting condition arises after the exit procedure has commenced, there shall be means to warn the user that setting has been prevented (for example: audible alert indication).

When setting is time dependent, means may be provided to override conditions preventing setting automatically.

The overriding of prevention of setting conditions shall be logged as specified in 8.10.

8.3.3.2 Exit route facility

Provision of an exit route facility is optional.

When an exit route facility is provided, the CIE shall be provided with means to select the defined alarm point(s) to be included in the exit route facility.

The CIE may provide the means to indicate that the exit procedure has commenced, in accordance with IEC 62642-1, 8.3.4 and Table 9.

8.3.3.3 Failure to set

Means shall be provided to indicate and/or notify when the CIE fails to set, following the initiation of setting procedure.

8.3.3.4 Set state

The CIE shall provide time limited means (for example, an output signal or message) to indicate that the system has set (in accordance with IEC 62642-1, 8.3.7).

Means shall be provided to comply with at least one of the requirements specified in IEC 62642-1, 8.3.7 whilst the I&HAS (or part thereof) is in the set state.

8.3.4 Unsetting procedure

The CIE shall provide means for a user to unset the I&HAS or part thereof in accordance with IEC 62642-1, 8.3.3 and 8.3.8.

NOTE It is not mandatory to provide means to unset a HAS or the HAS portion of an I&HAS.

The CIE may provide means to unset at pre-determined times. When this is done, the automatic unsetting action shall not cancel an existing alarm condition.

The procedures for unsetting with associated indications, including the optional use of an entry route, shall be in accordance with the requirements of IEC 62642-1, 8.3.8.

8.3.5 Restore function

The CIE shall provide means to restore conditions as defined in IEC 62642-1, 8.3.9.

8.3.6 Inhibit function

Inhibit functions may be applied to individual alarm, tamper, fault or hold-up points, as defined in IEC 62642-1, 8.3.10.

When the CIE is next set or unset, inhibit conditions shall be cancelled.

Where inhibit functions are provided, the manufacturer shall include details in documentation.

8.3.6.1 Automatic inhibit function

Inhibit may be performed automatically, except for hold-up functions.

Where this facility is provided, the manufacturer's documentation shall specify the number of occurrences of each type of event in a given set or unset period before the inhibit is applied.

8.3.7 Isolate operation

Isolate functions may be applied to individual alarm, tamper, fault or hold-up points; access to these means shall be restricted according to IEC 62642-1, 8.3.11.

8.3.8 Verification of I&HAS functions

The CIE shall include means for a user, at access level 2, to carry out a functional test of intrusion detectors and hold-up device(s), provided such tests do not render the device inoperable. Additionally, the CIE may include means to test WD or other components.

Tamper functionality is not the object of this test: the CIE shall continue to process tamper signals or messages as described in IEC 62642-1, 8.4.3 during such a test.

At grade 4, the CIE shall make provision for remote initiation of self-tests of system components, as required by the relevant component standards.

NOTE Display of information whilst in test condition is NOT considered to be an indication in the context of IEC 62642-1, Tables 8 and 9.

8.3.9 Alarm point soak test mode

In order to provide a tool for the maintenance of the I&HAS, the CIE may include a soak test function. When this is provided, alarm signals or messages from one or more alarm points under test shall continue to be recorded in the event log.

The soak attribute may be manually or automatically removed. The manufacturer's documentation shall specify the criteria for automatic removal of the soak test attribute and the time period for which it is applied (if not programmable). Access to initiate and manually restore the soak test function shall be restricted to access level 3 in all grades.

Indication that components are being soak tested shall be available to users at access levels 2 and 3 and the condition shall be indicated to a user when setting the system.

8.3.10 Other functions

In addition to normal functions described in this specification, the CIE may provide additional functions. A list shall be provided in the manufacturer's documentation.

8.4 Processing

The CIE shall include the means necessary to process input signals or messages and generate the output signals or messages, indications and notifications as required by IEC 62642-1, 8.4.

NOTE For the CIE to process internally generated fault conditions, it is assumed that the faults have not impaired the ability of the CIE to carry out this function.

8.4.1 Processing of input signals or messages

Intruder, hold-up, tamper and fault signals or messages shall be processed to provide the notifications required by IEC 62642-1, 8.4 and Table 7.

Dependent upon grade, masking and reduction of range of movement detector events shall similarly be processed according to IEC 62642-1, 8.4.3 or 8.4.4 and Table 7. The manufacturer's instructions shall state how masking and reduction of range signals or messages are processed.

8.4.1.1 Alarm inputs

Intrusion alarm signals or messages shall be processed

a) individually to generate one or more intruder alarm conditions, or

b) an alarm condition may be generated by the logical combination of signals or messages within a defined time window from the same alarm point or from logically grouped alarm points.

8.4.1.2 Priorities

The CIE default priority of signal or message processing shall be described in the manufacturer's documentation. In the event of multiple signals or messages being present simultaneously, all these signals or messages shall be processed and at least one of the highest priority signals or messages shall be notified as required by 8.6.

NOTE Multiple signals or messages from a single detector may be prioritised by that detector in accordance with the recommendation of the detector standard.

8.4.2 Processing of user inputs

When facilities are provided for a user to input commands other than at the CIE or ACE, processing shall verify that the selected functions are authorized according to 8.3.2.

8.4.3 Monitoring of CIE processing

In CIE with programme controlled data processing, means shall be provided to monitor the processing function and provide an appropriate signal, in accordance with Table 5.

A processing monitoring function shall be provided (for example: watchdog), which shall detect a complete failure of the processing function within 10 s and attempt to restart the processing.

If successful, the CIE shall resume operation in its previous operating mode (for example: set or unset) and this event shall be logged and indicated.

A dedicated output signal shall be provided which shall change state within 30 s of the processing failure being detected, unless the CIE has already resumed its previous operating mode after restart. Once activated, the output shall remain until the CIE has resumed its previous operating mode.

NOTE If cannot restart, I&HAS remains inactive.

Table 5 – Monitoring of processing

	Grade 1	Grade 2	Grade 3	Grade 4
Processing monitoring function	Op	Op	M	M
Processing failure output signal	Op	Op	Op	M
M = Mandatory Op = Optional				

8.5 Indication

8.5.1 General

Indications shall be provided and displayed in accordance with the requirements of IEC 62642-1, 8.5.1, 8.5.2 and 8.5.3.

The manufacturer shall document how a level 2, 3 or 4 user can cancel displayed information which is not permitted to be displayed at access level 1.

NOTE 1 This may be performed by an automatic timed operation.

The indications shown in Table 6 are additional to those shown in IEC 62642-1, Table 8.

Table 6 – Indications supplementary to those of IEC 62642-1

Indication	Grade 1	Grade 2	Grade 3	Grade 4
Failure of CIE processing (after successful restart)	Op	Op	M	M
Power output fault	Op	Op	M	M
Cause of prevention of setting	M	M	M	M
M = Mandatory Op = Optional				

When indicators share common means of annunciation, a pending indication shall be provided when further information is available for display (for example: a liquid crystal display).

Means shall be provided to control an alert indication for users at access level 1 to indicate that information is available to other access levels (for example: audible indicator or flashing visual indicator).

When an event activates more than one indication, at least one indication shall remain until the cause is restored.

NOTE 2 The pending and alert indications are described in IEC 62642-1.

NOTE 3 If a mimic panel is used, the indications may be available with no restriction to provide a tool for security management. In this case, according with the specific need of the installation, general access to the mimic panel should be restricted (for example: inside security room, inside key locked cabinet).

NOTE 4 Display of information whilst in a test mode is NOT considered to be an indication in the context of IEC 62642-1, Tables 8 and 9.

Masking and range reduction shall be indicated in the same way as intrusion or fault conditions, depending upon how they are processed. Depending upon how these conditions are reported by the detector, it may not be possible to differentiate between them at the CIE (see detector standards).

8.5.1.1 Alarm, tamper and fault indications

Alarm, tamper and fault indications shall require to be cancelled (acknowledgement) by a user according to the requirements of IEC 62642-1, 8.5.3.

8.5.1.2 Other conditions

Conditions other than alarm, tamper and fault shall be indicated during setting and unsetting and when required by a user.

8.5.2 Visual indicators

Where colours are used to differentiate the alarms, then the requirements of IEC 60073 shall apply.

8.5.3 Priority of indications

When indicators share common means of annunciation, indications shall be prioritised in accordance with the manufacturer's specifications.

8.6 Notification outputs

The CIE shall provide one or more output signals or messages to fulfil the requirements described in IEC 62642-1, 8.6. The CIE documentation shall state which option(s) can be fulfilled.

Additionally, if means is provided to gain level 3 access without level 2 authorisation (as permitted by IEC 62642-1, 8.3.1), means shall be provided to remotely notify "level 3 access" at security grades 2 and 3.

Where the CIE provides output signals or messages for SPT and WDs, means may be provided to delay or suppress the operation of WDs as described in IEC 62642-1, 8.6.

Means shall be provided to delay notification of an EPS fault for a maximum of 1 h. This notification shall be cancelled if the EPS fault has been restored within the delay period.

NOTE This should take into account the possibility of a delay being integrated into the SPT, this because some SPT may include a delay, hence it is advisable to make the delay introduced by the CIE programmable to avoid exceeding the maximum permitted.

8.6.1 Other notification

The CIE may provide other notification output signals or messages. Operation of such shall not affect any requirements of this standard.

8.7 Tamper security (detection/protection)

All connections to the CIE shall be contained within the CIE housing(s) and all connections to the ACE shall be contained within the ACE housing(s). The CIE and ACE housing(s) shall be provided with the means to prevent access to internal elements to minimize the risk of tampering, according to the grade of the CIE.

For the purposes of tamper protection and detection requirements, ACE are categorised as:

Type A: Access to internal elements resulting from damage to the housing could not enable the status of any part of the I&HAS to be changed or prevent the initiation of mandatory notification (for example: potted device);

Type B: Access to internal elements resulting from damage to the housing could enable the status of any part of the I&HAS to be changed or prevent the initiation of mandatory notification (for example: ACE includes connections for detectors).

8.7.1 Tamper protection

The construction of the CIE and ACE housing(s) shall meet the tamper protection requirements of IEC 62642-1 and the impact requirements for the appropriate grade according to Table 7. IK impact ratings are detailed in CEI 62262.

This requirement permits the housing to be damaged, provided that a tamper alarm shall be generated before unauthorised access to internal elements is possible (except for Type A devices).

Where the CIE is distributed within the housing of other components of the I&HAS, then the tamper protection of such housings shall comply with this standard.

Means of access to internal elements of a CIE or ACE shall be robust and mechanically secured.

Table 7 – Tamper protection

		Grade 1		Grade 2		Grade 3		Grade 4	
		Int	**Ext**	**Int**	**Ext**	**Int**	**Ext**	**Int**	**Ext**
CIE	Severity level (IK code) (design specification)	04	NA	06	NA	06	NA	06	NA
	Impact energy (Joule) (test condition)	0,5	NA	1	NA	1	NA	1	NA
ACE Type A	Severity level (IK code) (design specification)	04	07	04	07	04	07	04	07
	Impact energy (Joule) (test condition)	0,5	2	0,5	2	0,5	2	0,5	2
ACE Type B	Severity level (IK code) (design specification)	04	07	06	08	06	08	06	08
	Impact energy (Joule) (test condition)	0,5	2	1	5	1	5	1	5

NA = not applicable.
Int = inside the supervised premises.
Ext = outside the supervised premises (indoor or outdoor).

These requirements are not applicable to portable ACE.

In grades 1 and 2, this requirement does not include indicators or operating controls (for example: push-buttons, keypads, LCD or graphic screens); in grades 3 and 4, such indicators and operating controls are included, where these can be accessed by a level 1 user.

8.7.2 Tamper detection

Whether the CIE/ACE is self-contained within its own housing(s) or is distributed within the housing(s) of other components of the I&HAS, a tamper signal or message shall be generated according to the requirements specified in Table 8 before access can be gained to override the detection.

Table 8 – Tamper detection

Event to be detected	Grade 1	Grade 2	Grade 3	Grade 4
Access to the inside of the housing [a]	M	M	M	M
Removal from mounting	Op	Op	M	M
Removal from mounting (wire-free system components)	Op	M	M	M
Penetration of the housing [b]	Op	Op	Op	M
M = Mandatory Op = Optional NA = Not applicable. [a] Not applicable to Type A device. [b] When located outside the supervised premises. These requirements are not applicable to portable ACE.				

8.7.2.1 Access to the inside of housing

Opening the CIE/ACE type B housing by normal means shall generate a tamper signal or message.

The housing shall not permit the introduction of tools of dimensions as specified in Table 9 to defeat the tamper detection before it has operated.

Table 9 – Tool dimension for tamper detection

Tool	Grade 1	Grade 2	Grade 3	Grade 4
Steel rod as specified in CEI 60529, with diameter	2,5 mm	2,5 mm	1 mm	1 mm
Flat bar of dimension	10 × 1 × > 300 mm	10 × 1 × > 300 mm	5 × 0,5 × > 300 mm	5 × 0,5 × > 300 mm
Steel wire of tensile strength 650 - 825 MPa and dimensions	NA	NA	1 mm dia × 300 mm	1 mm dia × 300 mm
NA = Not applicable.				

This requirement is not applicable to type A devices.

In grades 1 and 2, this requirement does not include insertion of the tool via indicators or operating controls (examples are push-buttons, keypads, LCD or graphic screens) or other apertures; in grades 3 and 4 such indicators, operating controls and any other apertures accessible to a level 1 user are included.

8.7.2.2 Removal from mounting

Attempts to remove the CIE/ACE type B from its mounting surface for a distance greater than that defined in Table 10 shall generate a tamper signal or message according to Table 8.

It should not be possible to defeat the removal from mounting detection by sliding a 25 × 1 × > 300 mm blade or by use of pliers (of thickness 5 mm and reach 150 mm) between the mounting surface and the CIE/ACE.

Table 10 – Removal from mounting

	Grade 1	Grade 2	Grade 3	Grade 4
Maximum distance before tamper detected	10 mm	10 mm	5 mm	5 mm

8.7.2.3 Penetration of the housing

When mounted according to the manufacturer's instructions, it shall not be possible to penetrate the housing of the CIE/ACE type B through any of its accessible faces with a metal tool creating a hole of 4 mm or greater diameter without generating a tamper signal or message.

NOTE The aim is to detect a reduction of the original integrity of the housing. The definition of the hole diameter is to set an objective threshold for both product design and performance verification.

8.7.3 Monitoring of substitution

Grade 4 CIE shall provide means to monitor substitution of I&HAS components as required by IEC 62642-1, 8.7.3 and 8.7.4.

8.8 Interconnections

The CIE shall include means to verify that the interconnection function is operating normally as described in IEC 62642-1, 8.8 (including subclauses).

The CIE shall include physical and logical interface for interconnections. The manufacturer's documentation shall specify the type of the interconnection supported, as shown in Annex A.

NOTE 1 I&HAS component standards specify certain interconnection requirements.

NOTE 2 CEI 62642-5-3 specifies requirements for wire-free interconnections.

8.9 Timing

Signals and messages shall be processed as specified in IEC 62642-1, 8.9 (including subclauses).

Timings shall be applied to masking and reduction of range conditions according to whether they are processed as fault or intrusion events.

NOTE 1 Immunity to accidental recognition of an alarm signal or message due to electrical interference (e.g. EMI) is addressed by the EMC regionaldirective.

NOTE 2 Annex B includes a summary of the timing requirements.

8.10 Event recording

Event recording shall be in accordance with IEC 62642-1, 8.10.

NOTE The count of the number of events recorded from a single source during an unset period may be reset to zero in the event of an access level 3 restore operation.

The CIE shall include means to record the events as specified in Table 22 of IEC 62642-1 and, in addition, those conditions shown in Table 11.

Table 11 – Additional events to be included in event log

Events	Grade 1	Grade 2	Grade 3	Grade 4
Input device disabled for detection of repeated invalid authorisation codes	Op	M [a]	M	M
Failure of CIE processing (after successful restart)	Op	Op	M	M
Low battery, self-powered logical key	Op	M	M	M
Acknowledgement of low battery, self-powered logical key on setting	Op	M	M	M
Masking [b]	Op	Op	M	M

Events	Grade 1	Grade 2	Grade 3	Grade 4
Reduction of range [b]	Op	Op	Op	M
Identification of non-I&HAS interface used (see Annex C)	Op	M	M	M

M = Mandatory Op = Optional

[a] If option selected - see Table 4.

[b] "Reduction of range" may be indistinguishable from "Masking" (see CEI 62642-2 series).

8.10.1 Event recording at the CIE

When events are recorded at the CIE, each new event shall be recorded during the processing time permitted by IEC 62642-1, 8.9.2.

Recording of the events listed as mandatory in Table 11 and in IEC 62642-1, Table 22 shall not be affected, nor overwritten by the recording of events listed as "optional" (for example: separate event logs) where this will reduce the number of recorded events below the minimum required by IEC 62642-1, Table 21.

Logging of additional events, outside the scope of IEC 62642-1 is permitted, but shall not over-ride events specified by IEC 62642-1, Table 22 where this will reduce the number of recorded events below the minimum required by IEC 62642-1, Table 21.

The time recorded with a logged event shall include, as a minimum, hours and minutes, the date shall include as a minimum the day and month.

Where the storage time requirement of IEC 62642-1, Table 21 is met by the provision of a memory support battery, the CIE manufacturer shall specify the interval between battery changes.

In CIE for grades 3 and 4, a facility shall be provided to permanently record the event log.

NOTE It is not essential for the CIE to provide the means of permanently recording the event log, provided that it has the means to transfer the event log to an appropriate external device (for example: a printer).

8.10.2 Event recording at the ARC or other remote location

When event recording is provided at the ARC or other remote location, the CIE shall provide means to indicate that the transmission of events to the remote location has been unsuccessful.

When events cannot be transferred, in security grade 1, a fault condition shall be generated. In security grades 2, 3 and 4, events that have failed to be transmitted shall be transferred to a suitable I&HAS component for storage until transfer is possible. The requirements for this temporary memory shall be in accordance with the requirements of IEC 62642-1, Table 21.

8.11 Power supply

The CIE may be powered by an integrated PS or by a separate PS. In either case the requirements of IEC 62642-1, 9.2, EN 50131-6 and this standard shall be complied with.

The PS shall be capable of supporting the CIE in all conditions including when recharging storage devices within the required periods.

The manufacturer's documentation shall define the current consumption of the CIE and of the ACE.

NOTE The system designer (installer) will need to calculate the total stand-by period required for the I&HAS, according to the grade of the I&HAS, as indicated in IEC 62642-1.

9 Product documentation

9.1 Installation and maintenance

Information specified by IEC 62642-1, 14.2 shall be provided, along with the following:

a) operating temperature and humidity range;

b) weights and dimensions;

c) fixing details;

d) installation, commissioning and maintenance instructions, including terminal identifications;

e) type of interconnections (refer to 8.8);

f) details of methods of setting and unsetting possible (see 11.7.1 to 11.7.3 and Tables 23 to 26);

g) where there are serviceable parts (example: fuses) their type and value;

h) power supply requirement if no integrated PS;

i) where PS is integrated, the information required by EN 50131-6, Clause 6;

j) the maximum number of each type of ACE and expansion device;

k) the current consumption of the CIE and each type of ACE and expansion device, with and without an alarm condition;

l) the maximum current rating of each electrical output;

m) programmable functions provided;

n) how indications are made inaccessible to level 1 users when level 2, 3 or 4 user is no longer accessing the information (see 8.5.1);

o) masking/reduction of range signals/messages processed as “fault” or “masking” events (see 8.4.1, 8.5.1 and Table 11);

p) prioritisation of signal and message processing and indications (see 8.4.1.2, 8.5.3);

q) the minimum number of variations of PIN codes, logical keys, biometric keys and/or mechanical keys for each user (see 8.3);

r) method of time-limiting internal WD for level 3 access without level 2 authorisation (see 8.3.1);

s) the number and details of disallowed PIN codes (see 8.3.2.2.1);

t) details of any biometric authorization methods used (see 8.3.2.2.3);

u) the method used to determine the number of combinations of PIN codes, logical keys, biometric keys and/or mechanical keys (see 11.6);

v) number of invalid code entries before user interface is disabled (see 8.3.2.4);

w) details of means for temporary authorization for user access (see 8.3.2);

x) if automatic setting at pre-determined times provided, details of pre-setting indication and any automatic over-ride of prevention of set (see 8.3.3, 8.3.3.1);

y) details of conditions provided for the set state (see 8.3.3.4);

z) notification output signals or messages provided (see 8.6);

aa) other output configurations to interface with I&HAS components (see 8.2);

bb) criteria for automatic removal of “soak test” attribute (see 8.3.9);

cc) number of events resulting in automatic inhibit (see 8.3.6.1);

dd) if ACE is type A or type B (see 8.7) and whether portable or moveable (see 11.14);

ee) component data for non-volatile memory components (see Table 30, step 6);

ff) life of memory support battery (see 8.10.1);

gg) optional functions provided (see 4.1);

hh) additional functions provided (see 4.2, 8.1.8);

ii) access levels required to access such additional functions provided;

jj) details of any programmable facility that would render an I&HAS non-compliant with IEC 62642-1, 8.3.13 or compliant at a lower security grade, with instruction on consequent removal of compliance labelling (see 4.2 and 8.3.10).

9.2 Operating instructions

The following information shall be provided:

a) operating instructions for all security and non security functions available to the user;

b) standard(s) to which compliance is claimed for product;

c) security grade to which the CIE and ACE comply;

d) environmental class;

e) the minimum number of variations of logical and/or mechanical keys for each user;

f) the number and details of disallowed codes;

g) user programmable functions provided;

h) where there are user serviceable parts (example: fuses), their type and value.

10 Marking and labelling

The CIE and ACE shall be marked as required by IEC 62642-1, along with other information required by regional regulatory directives.

11 Tests

Where products are to be tested for compliance with this standard, the requirements of Clause 11 shall be applied.

Security grades 1 to 4 shall be in accordance with the descriptions in IEC 62642-1.

In the event of an additional component being developed for use with equipment already tested or of that equipment being revised, a revised test plan should be agreed with the test house.

11.1 Test conditions

11.1.1 Laboratory conditions and tolerance

Testing conditions shall be in accordance with IEC 60068-1:1988, 5.3.1, as follows:

– temperature: 15 °C to 35 °C

– relative humidity: 25 % to 75 %

– air pressure: 86 kPa to 106 kPa

11.1.2 Mounting

Except where shown otherwise, the CIE/ACE shall be mounted in accordance with the manufacturer's installation instructions. For environmental testing, the EUT shall be mounted in its correct operational orientation. The material used for the mounting surface shall not influence the test results.

Any additional equipment necessary to carry out the tests (for example: simulation of detectors or warning devices) shall be supplied by the manufacturer by agreement with the test house.

All input signals/messages (for example: directly wired detector inputs or bus line) shall be correctly terminated according to the manufacturer's instructions.

11.1.3 CIE test configuration

For functional testing, a CIE with representative configuration shall be supplied, as follows:

a) the CIE shall include at least one of each type of ACE and 10 % (but at least one) of each type of expansion device or networked CIE component for which the manufacturer requires the testing;

b) the manufacturer shall provide equipment to the test house with alarm point inputs connected as defined below and programmed to meet the requirements of this standard:

- each peripheral component capable of accepting inputs from alarm points shall have 10 % (but at least 2) of each type of input connected to alarm points;
- for wire-free equipment, at least 8 wire-free alarm points shall be tested;
- if either of the above determinations result in a number greater than the capacity of the device, all inputs shall be connected;
- where several "bus" inputs are provided or a mix of wired and wire-free inputs may be connected, the alarm points shall be distributed to check all buses and all types of interconnections;
- there may be several types of peripheral system components capable of accepting input connections. In this case, all such types of peripheral shall be checked;

c) the remainder of the I&HAS configuration may be simulated (for example: switches to simulate detectors, LEDs to simulate WDs);

d) the event log may be pre-filled by the manufacturer before the test.

The EPS and any APS shall be connected according to the manufacturer's instructions.

Where a real time clock is used in conjunction with an event log, the clock shall be set to the local time.

The manufacturer shall provide a declaration that the maximum system configuration for the CIE has been fully tested in-house.

A reduced system configuration may be provided for environmental and EMC testing.

11.1.4 Power supply

Where power for the CIE is provided by PS type A or B, the reduced functional test shall be carried out with the EPS at nominal value and with the APS at a level of at least 80 % of full capacity and connected according the manufacturer's instructions. For a CIE requiring a type C PS, the SD shall be at a level of at least at 80 % of full capacity.

11.1.5 Event log checks

Test procedures specify checking of event logs at the step to which the check is relevant. It may not be practical to perform the check at this step (for example: if CIE shall be in unset condition to view log events). Thus all log event checks for a test may be performed together as a final step.

At least one check should verify that the time specified in 8.10.1 is met.

11.1.6 Documentation

11.1.6.1 Product

The product documentation (as required in Clause 9) shall be provided with the CIE.

11.1.6.2 Simulator test device

If additional equipment (for example: a simulator or a programmable device) is supplied by the manufacturer, connection drawings, operational description and instructions for use shall be supplied.

11.2 Test procedures

All tests described in Clause 11 shall be carried out.

NOTE When features defined in this standard as optional are not provided then the testing is not required.

11.2.1 Tolerances

Where signals/messages are applied for a specified time, this shall be subject to a tolerance of –0 %, +5 %.

The pass-fail criteria are given in each test.

11.2.2 Wire-free devices

Wire-free devices shall be subjected to the additional tests required by IEC 62642-5-3.

11.3 Reduced functional test

For specified tests, (for example: environmental tests), it may not be possible or desirable to carry out a full functional test; in these cases a reduced functional test shall be carried out in accordance with Table 12.

Table 12 – Reduced functional test

Step	Test condition (c)	Action (d)	Measurement (e)	Pass/fail criteria (f)
1	CIE unset Absence of “intruder, tamper, fault signals and messages” No indication active	Apply an intruder alarm signal or message for 401 ms.	Check indications.	Indications shall be according to the grade (as shown in IEC 62642-1, Tables 8 and 9).
2	As above +: one intruder alarm input, not allocated as an “entry route”	Attempt to set the system.	Record whether the system sets.	The system should be prevented from setting.
3	As in 1 above	Set the system.	Record indications	Indications shall be according to the grade (as shown in IEC 62642-1, Tables 8 and 9).
4	CIE set	Apply an alarm signal or message as specified in 8.9.	Monitor the notification output signals or messages and record results.	At least one notification configuration required by IEC 62642-1, Table 10, according to the grade, shall be activated in accordance with IEC 62642-1, Table 7.
5	CIE in “set condition” and in “alarm” conditions	Manually unset the CIE.	Record whether the system has changed its status to “unset” and that the notification output signals or messages are correct and check the event log (grades 2, 3 and 4).	CIE unset Indications shall be according to the grade (as shown in IEC 62642-1, Tables 8 and 9). WD outputs shall silence, other notification output signals or messages may remain active until restored. Correct time and events sequences recorded
6	CIE in “unset condition”	Restore CIE.	Record whether system returns to normal condition.	In accordance with 8.3.5

11.4 Functional tests

11.4.1 Processing intruder alarm signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.1, 8.3.5, 8.4.1, 8.4.1.2, 8.5, 8.6, 8.9 and 8.10:

1) receive and process an intruder signal or message, within the processing timing requirements of this specification, when the CIE is in the set and the unset conditions;
2) provide indication(s) and notification(s);
3) correctly record the event(s) in the event log;
4) restore in accordance with 8.3.5.

b) Principle

The test consists of applying an intrusion signal/message as specified in 8.9 to an intruder input and monitoring that the input has been processed within the required time period and that the correct indication and notification(s) occur, see Table 13.

Table 13 – Tests of the processing of intruder signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.		GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied Time when notification occurs Record the event log.	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, Table 7 and 8.4.1. The indications and notifications shall be in accordance with IEC 62642-1, Tables 8, 9 and 10.
1	CIE in “set mode”	Apply intruder signal/message for 401 ms	General measurement + Record the identity of the alarm point being activated.	General criteria + Notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with alarm condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore (example: by entering a correct PIN number into the keypad)	General measurement	In accordance with 8.3.5
4	CIE in “set mode” NOTE To verify that multiple signals or messages applied at the same alarm point, are recorded in the event log the number of times specified in IEC 62642-1, 8.10.	Apply the same intruder signal/message for 401 ms once more than the maximum number of times specified in IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of intruder alarms from the same source shall comply with IEC 62642-1, 8.10.
5	CIE in “unset mode” NOTE To verify that intruder signals or messages are not recorded in the event log.	Apply the same intruder signal/message for 401 ms four times. Afterwards repeat step 3.	General measurement	General criteria
6	CIE in “set mode”. NOTE To verify that if multiple signals or messages are applied, at least one is processed correctly.	Apply intruder signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE or 5 (whichever is the greater) within 1 s.	General measurement	At least one intruder signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
7	CIE in “set mode“ (with more than one alarm condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.1.1.
8	CIE in “unset mode“	Restore all the conditions.	General measurement	In accordance with 8.3.5

11.4.2 Processing of hold-up signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE including hold-up function to comply with 8.1.2, 8.3.5, 8.4.1, 8.5, 8.6, 8.9, 8.10 and to:

1) receive and process a hold-up signal or message, within the processing timing requirements of this specification, when the CIE is in the set and the unset conditions;

   NOTE This test refers to the HAS portion of the CIE being set or unset. Where provision of an unset HAS mode is not provided, this portion of the test is not needed.

2) provide indication(s) and notification(s);

3) correctly record the event(s) in the event log;

4) restore in accordance with 8.3.5.

b) Principle

The test consists of applying a hold-up signal as specified in 8.9 or a hold-up message compatible to the CIE to a hold-up input when the system is in a variety of conditions shown in Table 14 below. The system shall be monitored to ensure that the input has been processed within the required time period and that the correct indication(s), notification(s) and event recording occur.

Table 14 – Tests of the processing of hold-up signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below, with all inputs and outputs in normal condition.		GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied Time when notification occurs Record the event log	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, Table 7 and 8.4.1. The indications and notifications shall be in accordance with IEC 62642-1, Tables 8, 9 and 10.
1	CIE in “set mode”	Apply hold-up signal/message for 401 ms.	General measurement + Record the identity of the alarm point being activated.	General criteria + As defined in 8.9, notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with alarm condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore	General measurement	In accordance with 8.3.5
4	CIE in “set mode” NOTE To verify that multiple signals or messages applied at the same hold-up alarm point, are recorded in the event log the number of times specified in IEC 62642-1, 8.10.	Apply the same hold-up signal/message for 401 ms once more than the maximum number of times specified in IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of hold-up alarms from the same source shall comply with IEC 62642-1, 8.10.
5	CIE in “unset mode” NOTE To verify that hold-up signals or messages are not recorded in the event log.	Apply the same hold-up signal/message for 401 ms four times. Afterwards repeat step 3.	General measurement	General criteria
6	CIE in “set mode” NOTE To verify that if multiple signals or messages are applied, at least one is processed correctly.	Apply hold-up signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE or 5 (whichever is the greater) within 1 s.	General measurement	At least one hold-up signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
7	CIE in “set mode“ (with more than one alarm condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.1.1.
8	CIE in “unset mode“	Restore all the conditions.	General measurement	In accordance with 8.3.5

11.4.3 Processing of tamper signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.3, 8.3.5, 8.4.1, 8.5, 8.6, 8.9, 8.10 and to:

1) receive and process a tamper signal or message, within the processing timing requirements of this specification, when the CIE is in the set and the unset conditions;
2) provide indication(s) and notification(s);
3) correctly record the event(s) in the event log;
4) restore in accordance with 8.3.5.

b) Principle

The test consists of applying a tamper signal as specified in 8.9 or a tamper message compatible with the CIE, to a tamper input when the system is in a variety of conditions shown in Table 15 below. The system shall be monitored to ensure that the input has been processed within the required time period and that the correct indication(s), notification(s) and event recording occur.

Table 15 – Tests of the processing of tamper signal or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below with all inputs and outputs in normal condition. When multiple methods to set and to unset the CIE are provided, then the test shall be carried out for each method.		GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied Time when notification occurs Record the event log	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, Table 7 and 8.4.1. The indications and notifications shall be in accordance with IEC 62642-1, Tables 8, 9 and 10.
1	CIE in “set mode”	Apply tamper signal/message for 401 ms	General measurement + Record the identity of the alarm point being activated.	General criteria + As defined in 8.9 notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with tamper alarm condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore	General measurement	In accordance with 8.3.5

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
4	CIE in “set mode” NOTE To verify that multiple tamper signals or messages from the same source are recorded in the event log the number of times specified in IEC 62642-1, 8.10.	Apply the same tamper signal/message for 401 ms once more than the maximum number of times specified in IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of tamper alarms from the same source shall comply with IEC 62642-1, 8.10.
5	CIE in “unset mode“	Apply tamper signal/message for 401 ms.	General measurement + Record the identity of the alarm point being activated	General criteria + As defined in 8.9 notification (grade dependent, see IEC 62642-1, Table 7) shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
6	CIE in “unset mode” NOTE To verify that multiple tamper signals or messages from the same source are recorded in the event log the number of times specified in IEC 62642-1, 8.10.	Apply the same tamper signal/message for 401 ms once more than the maximum number of times specified in IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of tamper alarms from the same source shall comply with IEC 62642-1, 8.10.
7	CIE in “set mode”. NOTE To verify that if multiple tamper signals or messages are applied, at least one is processed correctly.	Apply tamper signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE or 5 (whichever is the greater) within 1 s.	General measurement	At least one tamper signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
8	CIE in “set mode“ (with more than one tamper alarm condition)	Unset the CIE.	General measurement	General criteria Indications shall comply with 8.5.1.1.
9	CIE in “unset mode“	Restore all the conditions.	General measurement	In accordance with 8.3.5

11.4.4 Processing of fault signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.4, 8.3.5, 8.4.1, 8.5, 8.6, 8.9 and 8.10 to receive, process, log and notify a fault signal or message, within the requirements of this specification. The tests shall be performed with the CIE in set and unset modes to ensure that detection of faults satisfies all relevant requirements.

b) Principle

The principle consists of demonstrating the ability of the CIE to:

1) receive and process a fault signal or message, within the processing timing requirements of this specification, when the CIE is in the set and the unset conditions;
2) provide indication(s) and notification(s);

3) correctly record the event(s) in the event log;
4) restore in accordance with 8.3.5.

The test consists of applying fault conditions as specified in 8.1.4, as shown in Table 16.

The system shall be monitored to ensure that the input has been processed within the required time period and that the correct indication(s), notification(s) and event recording occur.

Table 16 – Test of processing of fault signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.	An EPS fault signal or message should be applied only where specifically stated.	GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied. Time when notification occurs. Record the event log.	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, Table 7 and 8.4.1. The indications and notifications shall be in accordance with IEC 62642-1, Tables 8, 9 and 10.
1	CIE in “set mode”	Apply fault signal or message for 10,1 s.	General measurement + Record the identity of the alarm point of the fault being activated.	General criteria + Notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with fault condition)	Unset the CIE.	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore	General measurement	In accordance with 8.3.5
4	CIE in “set mode” NOTE To verify that repetitive fault signals or messages are recorded in the event log as required by IEC 62642-1, 8.10	Apply the same fault signal or message for 10,1 s once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of fault alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.
5	CIE in “unset mode“	Apply fault signal or message for 10,1 s.	General measurement	General criteria
6	CIE in “unset mode” NOTE To verify that repetitive fault signals or messages are recorded in the event log as required by IEC 62642-1, 8.10.	Apply the same fault signal or message for 10,1 s once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of fault alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
7	CIE in “set mode”. NOTE To verify that if repetitive fault signals or messages are applied, at least one is processed correctly.	Apply 5 fault signals or messages (or the maximum possible number the EUT can recognize if less than 5) within 1 s.	General measurement	At least one fault signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
8	CIE in “set mode“ (with more than one fault condition)	Unset the CIE	General measurement	General criteria Indications shall comply with 8.5.
9	CIE in “unset mode“	Restore all the conditions.	General measurement	In accordance with 8.3.5
10	CIE in “set mode”	Apply at least one of each of intruder, hold-up, tamper and fault signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE or 5 (whichever is the greater) within 1 s.	General measurement + Record the identity of the intruder, hold-up, tamper and faults being activated.	General criteria + Notification should be in accordance with 8.4.1. All the conditions shall be correctly identified and logged in the event log at the correct time.
11	CIE in “unset” mode Enable EPS Fault notification delay required by 8.6.	Apply “EPS Fault” signal or message.	General measurement	Notification of the fault shall be delayed as required by 8.6.
12	As step 11, during delay period	Remove “EPS Fault” signal or message.	General measurement	Notification shall be cancelled according to 8.6.

11.4.5 Processing masking signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.6, 8.3.5, 8.5, 8.6, 8.9 and 8.10 to receive, process, log and notify a masking signal or message, within the requirements of this standard. The tests shall be performed with the CIE in set and unset modes to ensure that detection of faults satisfies all relevant requirements.

b) Principle

This test shall be processed as follows:

1) receive and process a masking signal or message as required by 8.1.6 and 8.10;
2) provide notification and indication(s);
3) correctly record the event(s) in the event log.

The test consists of applying masking signals or messages as specified in 8.1.6 and verifying that the correct indication and notification(s) occur, see Table 17.

Table 17 – Test of processing of masking signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.	* When processed as “intrusion”. If processed as “fault”, replace by “10,1 s”.	GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied Time when notification occurs Record the event log.	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, 8.4.5. The indications and notifications shall be in accordance with IEC 62642-1 Table 8 and 9. NOTE IEC 62642-1 permits masking events to be processed either as “fault” or as “intrusion” response.
1	CIE in “set mode”	Apply masking signal or message for 401 ms *.	General measurement Record the identity of the device being activated.	General criteria Notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with masking condition)	Unset the CIE.	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore.	General measurement	In accordance with 8.3.5
4	CIE in “set mode” NOTE To verify that repetitive masking signals or messages are recorded in the event log as required by IEC 62642-1, 8.10.	Apply the same masking signal or message for 401 ms * once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of masking alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.
5	CIE in “unset mode“	Apply masking signal or message for 401 ms *.	General measurement	General criteria
6	CIE in “unset mode” NOTE To verify that repetitive fault masking signals or messages are recorded in the event log as required by IEC 62642-1, 8.10.	Apply the same masking signal or message, as specified in 8.9 once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of masking alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.
7	CIE in “set mode”. NOTE To verify that if repetitive masking signals or messages are applied, at least one is processed correctly.	Apply 5 masking signals or messages (or the maximum possible number the EUT can recognize if less than 5) within 1 s.	General measurement	At least one masking signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
* When processed as “intrusion”. If processed as “fault”, replace by “10,1 s”.				

11.4.6 Processing reduction of range signals or messages

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.7, 8.3.5, 8.5, 8.6, 8.9 and 8.10 to receive, process, log and notify a reduction of range signal or message, within the requirements of this standard. The tests shall be performed with the CIE in set and unset modes to ensure that detection of faults satisfies all relevant requirements.

b) Principle

The test shall be processed as follows:

1) receive and process a masking signal or message as required by 8.1.7 and 8.10;
2) provide notification and indication(s);
3) correctly record the event(s) in the event log.

The test consists of applying reduction of range signals or messages as specified in 8.1.7 and verifying that the correct indication and notification(s) occur, see Table 18.

Table 18 – Test of processing of reduction of range signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.	* When processed as “intrusion”. If processed as “fault”, replace by “10,1 s”.	GENERAL MEASUREMENT Record the condition of the indications and notifications of the CIE and any associated user input devices (for example: remote keypads). Time when signal/message applied. Time when notification occurs. Record the event log	GENERAL CRITERIA Processing shall be in accordance with IEC 62642-1, 8.4.6. The indications and notifications shall be in accordance with IEC 62642-1, Tables 8, 9 and 10. NOTE IEC 62642-1 permits reduction of range events to be processed EITHER as “fault” or as “intrusion” response.
1	CIE in “set mode”	Apply reduction of range signal or message for 401 ms *.	General measurement Record the identity of the device being activated.	General criteria Notification shall occur within the time specified by IEC 62642-1, 8.9. The logging shall be in accordance with 8.10.
2	CIE in “set mode“ (with reduction of range condition)	Unset the CIE.	General measurement	General criteria Indications shall comply with 8.5.
3	CIE in “unset mode“	Restore.	General measurement	In accordance with 8.3.5

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
4	CIE in “set mode” NOTE To verify that repetitive reduction of range signals or messages are recorded in the event log as required by IEC 62642-1, 8.10.	Apply the same reduction of range signal or message for 401 ms * once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of reduction of range alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.
5	CIE in “unset mode“	Apply reduction of range signal or message for 401 ms *.	General measurement	General criteria
6	CIE in “unset mode” NOTE To verify that repetitive reduction of range signals or messages are recorded in the event log as required by IEC 62642-1, 8.10.	Apply the same reduction of range signal or message for 401 ms * once more than the maximum permitted by IEC 62642-1, 8.10. Afterwards repeat step 3.	General measurement	The number of reduction of range alarms recorded from the same source shall be as specified in IEC 62642-1, 8.10.
7	CIE in “set mode” NOTE To verify that, if repetitive reduction of range signals or messages are applied, at least one is processed correctly.	Apply 5 masking reduction of range signals or messages (or the maximum possible number the EUT can recognize if less than 5) within 1 s.	General measurement	At least one reduction of range signal or message shall be processed in accordance with 8.4.1.2 and 8.9.
* When processed as “intrusion”. If processed as “fault”, replace by “10,1 s”.				

11.4.7 CIE processing in the presence of non-I&HAS inputs

Processing of mandatory signals or messages in the presence of non-I&HAS signals or messages.

a) Object of the test

The object of the test is to demonstrate the ability of CIE that includes inputs for non-I&HAS purposes to comply with 8.1.8, 8.9 and 8.10; to receive and process an intruder, hold-up, tamper or fault signal or message within the processing timing requirements of this specification, when the CIE is in the set and the unset modes and one or more optional signals or messages are present.

b) Principle

The test consists of applying a mandatory signal or message, whilst a non-I&HAS signal or message is applied to another input of the CIE and monitoring that the mandatory signal or message has been processed within the required time period and that the correct indication and notification(s) occur. See Table 19.

Table 19 – Test of CIE processing in the presence of non-I&HAS inputs

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	CIE in “unset mode”	Apply an optional signal or message to the input(s) of the CIE. Within 500 ms after applying the optional signal or message apply a mandatory signal or message to an input of the CIE	Record: - the status of the notification outputs - the time period between the input of the mandatory signal or message and the initiation of the mandatory notification	Notification, arising from the input of the mandatory signals or messages, shall be initiated within the time specified by IEC 62642-1, 8.9.
2	CIE in “set mode”	Repeat as above.	As above	As above

11.5 Access level

11.5.1 Access to the functions and controls

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.1.5, 8.3.1, 8.3.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.2 and 8.10 to provide up to four levels of access and verify the relevant access to the functions and controls.

b) Principle

The test consists of attempting to use the functions and the controls required by 8.1.5, 8.3.1, 8.3.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.2 and 8.10, operating the CIE at each access level and verifying that access is granted for permitted functions and is denied for non-permitted functions (see Table 20).

Table 20 – Test of the access to the functions and controls

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	The CIE and any necessary ACE shall be mounted according to the manufacturer’s specifications.	At access level 1 attempt to operate all the functions and controls listed in 8.3.6, 8.3.7 and 8.3.9 and in IEC 62642-1, Tables 2, 5, 6 and 8 and 8.3.10.	Record whether access is permitted.	Access is in accordance with 8.3.9 and IEC 62642-1, Tables 2, 5, 6 and 8.
2	As above	Repeat as step 1 for access level 2.	As above	As above
3	As above	Repeat as step 1 for access level 3.	As above Record whether level 2 authorization for level 3 access is “until manually removed” or “required for each occasion”	As above
4	As above	Repeat as step 1 for access level 4.	As above	As above
NOTE If means is provided to gain level 3 access without level 2 authorisation (see IEC 62642-1, 8.3.1), not permitted at grade 4:				

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
5	CIE unset	Enter level 3 access code or key	Monitor outputs.	Notified by internal WD and (grade 2 and 3) remotely
6	Perform action defined by manufacturer to silence WD or allow to time out, as applicable	-	Monitor outputs and status.	WD silenced. Level 3 access obtained
7	CIE set	Repeat steps 5 and 6	Monitor outputs and status.	No response, remains at level 1 access

11.6 Authorization requirements

Where a CIE is able to accept more than one method of authorization, the number of combinations shall be checked individually for each method as per the following procedures, to ensure compliance if that method only is used on an I&HAS.

11.6.1 Mechanical key tests

a) Object of the test

The object of the test is to verify the mechanical key variations, as specified in IEC 62642-1, Table 3, are met by the CIE and any associated ACE and that the requirements of 8.3.2 and 8.3.2.1 are met.

The object of the test is also to verify the manufacturer's documentation complies with the requirements of Clause 9.

b) Principle

The test consists of verifying that the range of combinations of mechanical keys is provided and that invalid mechanical keys are not accepted.

c) Test conditions

The manufacturer shall provide the test-house with the following information:

1) the number of key variations;
2) the method used to determine the number of key variations.

d) Test procedure

The test shall be processed as follows:

1) Attempt to change the state of the CIE using a valid key.
2) Attempt to change the state of the CIE using a non valid key.
3) Examine the manufacturer's information regarding key construction and calculations.

e) Measurement

1) Verify that the manufacturer's information and calculations are valid.
   Note the state of the CIE before and after use of valid key.
2) Note the state of the CIE before and after attempted use of non-valid key.
3) Record details of the invalid keys.

f) Pass/fail criteria

1) The valid key changes the state of the CIE.

2) The non-valid key does not change the state of the CIE.

3) The manufacturer's supplied information and calculations verify that the number of combinations complies with IEC 62642-1, Table 3.

11.6.2 Logical key tests

Where no specific tests are provided for the type of logical key used, the principles of the "digital key" tests should be applied.

11.6.2.1 Digital key tests

a) Object of the test

The object of the test is to verify the number of logical key variations, as specified in IEC 62642-1, Table 3, are met by the CIE and any associated ACE and that the requirements of 8.3.2 and 8.3.2.2.2 are met.

The object of the test is also to verify the manufacturer's documentation complies with the requirements of Clause 9.

b) Principle

The test consists of verifying that the range of variations of digital keys are provided and that invalid digital keys are not accepted, also, where applicable, that copy rejection and power supply requirements are met.

c) Test conditions

The manufacturer shall provide the test-house with the following information:

1) The number of key variations.

2) The method used to determine the number of key variations.

3) If the operational range of the digital key exceeds 1 m, the method of rejection of unauthorised copies.

d) Test procedure

1) Attempt to change the state of the CIE using a valid digital key.

2) Attempt to change the state of the CIE using a non valid digital key.

3) Examine the manufacturer's information regarding digital key construction and calculations.

4) Check the number of variations of the digital key.

5) If the operational range exceeds 1 m, either
the manufacturer shall provide the means to simulate a copied key or
the manufacturer shall provide details of how the copy rejection operates.

6) If self-powered, the manufacturer shall provide the means to simulate a key with low storage device charge, as required by EN 50131-6, 7.7.4.1.

e) Measurement

1) Verify that the manufacturer's information and calculations are valid.

2) Note the state of the CIE before and after use of valid digital key.

3) Note the state of the CIE before and after attempted use of non-valid digital key.

4) Record details of the invalid digital keys.

5) Record range of digital key.

6) Record the system response to a copied key or
evaluate the manufacturer’s documented copy rejection technique.

7) Record the system responses to a key with low voltage storage device.

f) Pass/fail criteria

1) The valid digital key changes the state of the CIE.

2) The non-valid digital key does not change the state of the CIE.

3) The manufacturer's supplied information and calculations verify that the number of combinations complies with IEC 62642-1, Table 3.

4) If range exceeds 1 m, a copied key is rejected or
the manufacturer’s described copy protection technique meets the copy protection requirement.

5) If self-powered, the requirements of 8.3.2.2.2 and EN 50131-6, 7.7.4.1 for low battery reporting are met.

11.6.2.2 PIN code tests

a) Object of the test

The object of the test is to verify the number of combinations specified in IEC 62642-1, Table 3 are met by the CIE and any associated ACE and that the requirements of 8.3.2 and 8.3.2.2.1 are met.

The object of the test is also to verify the manufacturer’s documentation complies with the requirements of Clause 9.

b) Principle

The test consists of verifying that the range of variations of PIN codes is provided and that invalid codes are not accepted.

c) Test conditions

For the test purpose, the manufacturer shall provide to the test-house the following information:

1) the number of disallowed codes;

2) the method used to determine the number of variations;

3) for each user, the minimum number of variations of logical key shall be indicated.

d) Test procedure

1) Create samples of valid codes as described in the CIE documentation. The number of valid codes to be created shall be: 10 for grade 1; 20 for grade 2; 50 for grade 3; 100 for grade 4.

2) Attempt to create an invalid code.

3) Verify the validity of the manufacturer’s calculations.

e) Measurement

1) Record the valid codes.

2) Record the invalid code.

f) Pass/fail criteria

1) All valid codes created in “d) 1)” above shall be accepted according to grade.

2) Invalid codes shall not be accepted.

3) Calculations shall be shown to be in accordance with code combinations shown in Table 2.

11.6.2.3 Tests for authorization by biometric means

Relevant parts of the test procedure described for digital keys at 11.6.2.1 shall be applied.

Additionally, the manufacturer shall provide information for the test house to evaluate compliance with the requirements of 8.3.2.2.3 (Table 2).

11.6.2.4 Tests for authorization by combinations of keys

Where combinations of keys are accepted, as specified in 8.3.2.4, each type shall be evaluated as appropriate to the type of key. The timing requirements of Table 3 shall be met. The number of combinations of each type shall be multiplied to assess compliance with IEC 62642-1, Table 3.

11.6.3 Invalid authorization attempts

a) Object of the test

Verify that the detection and notification of attempted entry of invalid logical keys or (when the CIE has the means to distinguish such) mechanical keys complies with 8.3.2 and Table 3.

b) Principle

The test consists of entering a series of invalid logical or (if appropriate) mechanical keys and establishing that when the number of invalid attempts have been made as specified in Table 3 the user input device is disabled and/or a tamper signal or message is generated and recorded in the event log as specified. See Tables 21 and 22.

When testing invalid PIN codes, at least one attempt shall take the form of a valid code entry not completed within 60 s.

Table 21 – Test for disabling user input device by invalid keys

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
Repeat for each type of invalid attempt – i.e. PIN code, digital key, biometric key and (if the CIE has the means to identify such) mechanical key				
If the CIE has the facility to disable user input device carry out this series of tests				
	GENERAL: The CIE shall be configured with its inputs and outputs in their normal condition, allowing the CIE to be set and alarms to be generated from at least 1 alarm point.	GENERAL: The steps 2, 4, 5, 6 and 7 shall be repeated in the "UNSET" mode of the CIE.		
1	CIE unset	Enter a valid key and attempt to set CIE.	Record status of CIE.	CIE set
2	CIE set	Enter a series of invalid keys according to Table 1 to attempt to initially disable the user input device.	Record status of CIE, disabling of user input device, tamper conditions and event log.	CIE should not change state, the user input device shall be disabled, the generation of tamper conditions and event log shall be in accordance with Table 1.

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
3	CIE set	During the “disabling time” apply an alarm signal or message.	Record whether the alarm condition is processed.	The alarm generated during the disable period shall be processed in accordance with IEC 62642-1, Table 7 and 8.4.1.
4	CIE set	During the “disabling time” try to enter a valid key.	Record whether user input device responds to operation.	The CIE shall not change state. The user input device shall remain disabled.
5	CIE set	When disabling time has expired, enter another series of invalid keys according to Table 4.	Record status of CIE, disabling of user input device, tamper conditions and event log.	The CIE shall not change state and shall be in accordance with Table 4.
6	CIE set	During the “disabling time” try to enter a valid key.	Record whether user input device is available.	The CIE shall not change state. The user input device shall remain disabled.
7	CIE set	When disabling time has expired enter a valid key and attempt to change state of the CIE.	Record status of the CIE.	The CIE shall change state.

Table 22 – Test for generation of tamper signal or message by invalid keys

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
If the CIE has the facility in accordance with Table 1 to generate a tamper signal or message, carry out this series of tests				
	GENERAL: The CIE shall be configured with its inputs and outputs in their normal condition, allowing the CIE to be set and alarms to be generated from at least 1 alarm point.	GENERAL: The steps 2 and 3 shall be repeated in the “UNSET” mode of the CIE.		
1	CIE unset	Enter a valid key and attempt to set CIE.	Record status of CIE.	CIE set
2	CIE set	Enter a series of invalid keys according to Table 4 to attempt to generate a tamper condition.	Record status of CIE, tamper conditions and event log.	CIE shall not change state, the generation of tamper conditions and event log shall be in accordance with Table 1.
3	CIE set	Enter a valid key to acknowledge the tamper condition.	Record status of CIE, tamper conditions and event log.	The tamper condition shall be acknowledged and shall be in accordance with Table 1.

11.7 Operational tests

11.7.1 Setting procedures

a) Object of the test

The test consists of verifying that that all setting procedures are in accordance with 8.3.3, 8.3.3.2 and 8.3.3.3.

b) Principle

The test consists of setting the CIE and verifying that these are in accordance with the requirements of this standard (see Table 23).

Table 23 – Test of setting procedure

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in "unset" condition For the purpose of this series of tests, the keys and/or codes shall be selected to have the necessary authorisations for "inhibit" and "override" functions.		GENERAL: Record the CIE condition	GENERAL CRITERIA When the CIE fails to set, means shall be provided to indicate or notify. If the indication of the set state is provided, it shall be time-limited according to IEC 62642-1, 8.3.7. The logging shall be in accordance with 8.10.
Complete the following series of tests for each setting method given in the manufacturer's documentation.				
1	CIE is unset	Initiate exit procedure.	Record the CIE condition.	The CIE shall set and indicate accordingly.
2	CIE unset	Setting procedure initiated but prevented from completion "Fail to set" time expires	Record the CIE condition.	Incomplete exit condition indicated and/or notified, according to 8.3.3.3 CIE not set No alarm notification
For CIE where setting using exit route is possible, verify that means exists to select alarm points to be included in exit route facility and:				
3	CIE unset	Start the setting procedure (exit time).	Record the CIE condition.	The setting procedure shall be initiated and indicated according to 8.3.3.2 and IEC 62642-1, Tables 8 and 9.
4		Activate an exit route alarm point, during the exit time period.	Record the CIE condition.	The activated alarm point shall not cause alarm notification.
5		Ensure the alarm point is no longer in the activated condition. Allow the setting procedure to complete or complete setting procedure as appropriate to method.	Record the CIE condition.	The setting procedure shall be completed. CIE is set, in accordance with 8.3.3.2.
6	CIE unset Exit procedure initiated Exit route alarm point activated	Exit route alarm point remains activated Exit time or "Fail to set" time expires	Record the CIE condition.	Incomplete exit condition indicated and/or notified, according to 8.3.3.3 CIE not set No alarm notification
For CIE including facility to set by level 1 access, as permitted by IEC 62642-1, 8.3.4 (grade 1 only):				
7	CIE is unset	Initiate level 1 setting in accordance with manufacturer's instructions.	Record CIE action.	The CIE operation shall commence setting procedure.

Table 23 *(continued)*

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
8	During setting procedure	Operate level 1 "cancel setting" in accordance with manufacturer's instructions.	Record CIE action.	The CIE shall cancel the setting procedure and remain unset.
9	CIE is unset	Initiate level 2 setting in accordance with manufacturer's instructions.	Record CIE action.	The CIE operation shall commence setting procedure.
10	During setting procedure	Operate level 1 "cancel setting" in accordance with manufacturer's instructions.	Record CIE action.	The CIE shall continue the setting procedure. Allow to set.
11	CIE is set	Operate level 1 "cancel setting" in accordance with manufacturer's instructions.	Record CIE action.	The CIE shall remain set.

11.7.2 Prevention of setting and overriding of prevention of setting procedures

a) Object of the test

The test consists of verifying that all procedures are in accordance with 8.3.3.1.

b) Principle

The test consists of attempting setting the CIE and verifying that the responses are in accordance with the requirements of this standard (see Table 24).

Table 24 – Test of prevention of setting and overriding of prevention of setting procedure

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in "unset" condition. For the purpose of this series of tests, the keys and/or codes shall be selected to have the necessary authorisations for "inhibit" and "override" functions.	Provision of override of prevention of setting function and inhibit function described in the test are not mandatory (8.3.3.1 and 8.3.6).	GENERAL: Record the CIE condition.	GENERAL CRITERIA When the CIE fails to set, means shall be provided to indicate or notify. If the indication of the set state is provided, it shall be time-limited according to IEC 62642-1, 8.3.7. The logging shall be in accordance with 8.10.
Complete the following series of tests for each setting method given in the manufacturer's documentation and for each condition specified in IEC 62642-1, Table 4.				
1	Alarm point (not allocated to an exit route) in active condition CIE unset	Try to set the system.	Record the CIE condition.	The setting procedure shall be in accordance with 8.3.3 and IEC 62642-1, Table 4.

Table 24 *(continued)*

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
2	Alarm point (not allocated to an exit route) in active condition. Setting prevented (see step 1) CIE unset	Inhibit the active alarm point (if function provided) – see 8.3.6. Try to set the system.	Record the status of the CIE.	The setting procedure shall continue in accordance with IEC 62642-1, Table 4 and be completed according to manufacturer's instructions.
3	The CIE in "unset" condition. Tamper signal or message applied to the CIE	Try to set the system.	Record the status of the CIE.	The setting procedure shall be prevented in accordance with IEC 62642-1, Table 4
4	Setting prevented (see step 3) CIE unset	Override the tamper signal or message (if function provided) – see IEC 62642-1 Table 5. Try to set the system.	Record the status of the CIE.	The setting procedure shall continue in accordance with IEC 62642-1, Table 4 and be completed according to manufacturer's instructions.
5	The CIE is in "unset" condition. Hold-up signal or message applied to the CIE	Try to set the system.	Record the CIE condition.	The setting procedure shall be prevented in accordance with IEC 62642-1, Table 4.
6	Setting prevented (see step 5) CIE unset	Inhibit the hold-up device (if function provided) – see 8.3.6. Try to set the system.	Record the CIE condition.	The setting procedure shall continue in accordance with IEC 62642-1, Table 4 and be completed according to manufacturer's instructions.
For movement detector masking, movement detector range reduction and each fault signal or message specified in IEC 62642-1, Table 4 repeat steps 7 and 8.				
7	The CIE is in "unset" condition. Apply fault signal or message to CIE.	Try to set the system.	Record the CIE condition.	The setting procedure shall be prevented in accordance with IEC 62642-1, Table 4.
8	Setting prevented (see step 7) CIE unset	Override the setting prevention (if function provided) – see 8.3.6.	Record the CIE condition.	The setting procedure shall continue in accordance with IEC 62642-1, Table 4 and be completed according to manufacturer's instructions.

11.7.3 The set state

Prior to testing unsetting functions, ascertain from manufacturer's documentation which option(s) for the set state are provided (see 8.3.3.4).

At least one of the options described in IEC 62642-1, 8.3.7 shall be provided, appropriate to security grade.

Depending upon the option(s) provided, the relevant portion(s) of 11.7.4 shall be tested.

11.7.4 Unsetting procedures

a) Object of the test

Verify that all procedures are in accordance with the requirements of 8.3.4.

b) Principle

The test consists of unsetting the CIE using all the procedures provided as specified in the manufacturer's documentation and verification that these are in accordance with the requirements within this specification (see Table 25).

Table 25 – Test for unsetting procedure

Step	Test condition (c)	Procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in "set" condition. The keys and the codes used are all valid with the necessary authority.		GENERAL: Record the CIE condition.	GENERAL CRITERIA The indication of the unset state shall be time-limited according to IEC 62642-1, 8.3.8.2. The logging shall be in accordance with 8.10.
Complete the following series of tests for each unsetting method provided in the manufacturer's documentation.				
1	CIE set, in a normal condition with no alarms or, tamper signals or messages activated.	Try to manually unset the system.	Record the CIE condition.	The unsetting procedure shall be completed.
2	CIE set Alarm point (not on an agreed entry route) in active condition	Try to manually unset the system.	Record the CIE condition.	The unsetting procedure shall be completed. Notification, indication and event recording shall comply with IEC 62642-1, Tables 7, 8, 9 and 22.
For CIE with entry route facility, complete the following series of tests for each unsetting method provided in the manufacturer's documentation.				
3	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition. Record indication.	The unsetting procedure shall be initiated. Indication shall be in accordance with IEC 62642-1, 8.3.8.2 and Tables 8 and 9 and recorded in the event log in accordance with IEC 62642-1, Table 22.
4	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition.	The unsetting procedure shall be initiated.
5		Generate an intruder alarm from an entry route alarm point.	Record the CIE condition.	An intruder alarm shall not be notified.
6		Do not complete the unsetting procedure (let the entry time expire).	Record the CIE condition.	An alarm condition shall be notified according to IEC 62642-1, 8.3.8.2.
7	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition. Record indication.	The unsetting procedure shall be initiated. Indication shall be in accordance with IEC 62642-1, 8.3.8.2 and Tables 8 and 9.

Step	Test condition (c)	Procedure (d)	Measurement (e)	Pass/fail criteria (f)
8	Unsetting procedure in process	Generate an intrusion alarm from an entry route alarm point and complete the entry procedure.	Record the CIE condition Record indication and notification	CIE is unset. The intruder alarm shall not be processed. A correct entry procedure shall be indicated as per IEC 62642-1, 8.3.8.2 and Tables 8 and 9,and recorded in the event log in accordance with IEC 62642-1, Table 22.
9	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition.	The unsetting procedure shall be initiated.
10		Generate a tamper alarm from an entry route alarm point.	Record the CIE condition.	The tamper alarm shall be notified.
11	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition.	The unsetting procedure shall be initiated.
12		Generate an intrusion alarm from a non-entry route alarm point.	Record the CIE condition.	Indication or warning device shall be activated in accordance with IEC 62642-1, 8.3.8.2.
13	Unsetting is proceeding	Wait for expiry of time programmed or specified by manufacturer after indication or internal WD activated. MINIMUM time is 30 s	Record the CIE condition.	Where remote notification devices are connected, ensure this is not activated prior to the completion of the delay required by IEC 62642-1, 8.3.8.2.
14	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition.	The unsetting procedure shall be initiated.
15		Do not complete the unsetting procedure (let the entry time expire).	Record the CIE condition.	The alarm shall be notified in accordance with IEC 62642-1, 8.3.8.2.
16	CIE set	Manually start the unsetting procedure (entry time).	Record the CIE condition.	The unsetting procedure shall be initiated.
17		Generate an alarm from a non entry route alarm point.	Record the CIE condition.	Indication or warning device shall be activated in accordance with IEC 62642-1, 8.3.8.2.
18		Complete the unsetting procedure before the notification delay expires, see paragraph 3 of IEC 62642-1, 8.3.8.2.	Record the CIE condition.	The indicator or warning devices shall be restored and remote notification shall not take place. The CIE shall be unset.

11.7.5 Setting and/or unsetting automatically at pre-determined times

If the CIE has the facility to set and/or unset automatically at pre-determined times, the following test shall apply:

a) Object of the test

The test consists of verifying that all procedures are in accordance with 8.3.3, 8.3.3.1 and 8.3.4.

b) Principle

The test consists of attempting setting the CIE and verifying that the responses are in accordance with the requirements of this standard (see Table 26).

Table 26 – Test of setting and/or unsetting automatically at pre-determined times

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in "unset" condition. For the purpose of this series of tests, the keys and/or codes shall be selected to have the necessary authorisations for "inhibit" and "override" functions.	Provision of override of prevention of setting function and inhibit function described in the test are not mandatory (8.3.3.1 and 8.3.6).	GENERAL: Record the CIE condition.	GENERAL CRITERIA When the CIE fails to set, means shall be provided to indicate or notify. If the indication of the set state is provided, it shall be time- limited according to IEC 62642-1, 8.3.7. The logging shall be in accordance with 8.10.
If CIE has facility for setting automatically:				
1	CIE is unset, prior to time that pre-setting indication is scheduled.	Allow automatic sequence to operate.	Monitor indications and CIE status.	Pre-setting indication available as documented manufacturer. Setting and override of prevention of set shall be entered in event log.
2	With CIE set, create alarm.	Allow automatic unset to take place.	Monitor status and indications.	Unsetting takes place as scheduled. Alert indication present. Unsetting entered in event log
3		Obtain level 2 access.	Record displayed information.	Correct record of alarm created whilst set. Alarm is present in event log.
4	CIE is unset, prior to time pre-setting indication is scheduled. Condition to prevent setting present	Allow automatic sequence to operate.	Monitor indications and CIE status.	Pre-setting indication available as documented manufacturer. Setting prevented or prevention of setting automatically overridden. Setting and override of prevention of set shall be entered in event log.
If CIE has provision for automatic unsetting:				
5	CIE set	Initiate unsetting sequence in accordance with manufacturer's instructions.	Record the CIE condition.	The unsetting procedure shall be completed.
6	CIE set and in alarm condition	Initiate unsetting sequence in accordance with manufacturer's instructions	Record the CIE condition.	The unsetting procedure shall be completed. The alarm condition shall not be cancelled. Alarm event and unsetting shall be entered in event log.

11.7.6 Inhibit and isolate functions

a) Object of the test

The test consists of verifying that the operation of inhibit or isolate functions comply with the requirements of 8.3.6 and 8.3.7.

NOTE These tests are applicable only if one or both of these functions are provided.

b) Principle

The test consists of operating inhibit and isolate modes to ensure correct functionality (see Table 27).

c) Test condition

Examine the manufacturer's documentation to confirm details of functionality.

The test shall be run with the system initially in the unset condition.

Table 27 – Inhibit and isolate functions

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f) NOTE IEC 62642-1, Table 22 defines the event log information required and grade dependency.
INHIBIT FUNCTION			
1	Set the system, inhibiting an alarm point as described by manufacturer.		
2	Apply a signal or message to the inhibited input for the minimum time required to trigger, according to type.	Monitor the notification outputs.	Event log shall record the inhibit. There shall be no notification or log event for an alarm condition.
3	Unset the system and set it again.		
4	Apply a signal or message to the previously inhibited input for the minimum time required to trigger, according to type.	Monitor the notification outputs.	Notification and event log shall show normal (uninhibited) response.
5	Repeat steps, using a hold-up alarm point.	Monitor the system responses.	It shall not be possible to inhibit a hold-up alarm point.
ISOLATE FUNCTION			
6	Isolate an alarm point as described by the manufacturer.		Isolation shall be possible only at the specified access level(s). Event log shall record the isolation.
7	Set the I&HAS.		
8	Apply a signal or message to the isolated input for the minimum time required to trigger, according to type.	Monitor the system responses.	There shall be no notification or log event for an alarm condition.
9	Unset the system and set it again.		
10	Repeat step 8.	Monitor the system responses.	There shall be no notification or log event for an alarm condition.
11	Reinstate the alarm point as described by the manufacturer.		Reinstatement shall be possible only at the specified access level(s).
12	Repeat step 8.	Monitor the system responses.	Notification and event log shall show normal (reinstated) response.

11.7.7 Test functions

a) Object of the test

The object of the test is to verify the ability of the CIE to permit test functions to be carried out in accordance with the requirements of 8.3.8, 8.3.9 and 8.10.

b) Principle

The test consists of operating the test modes to ensure correct functionality (see Table 28).

c) Test condition

The test shall be run with the system initially in the unset condition.

Table 28 – Verification of test functions

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	With the system unset and in the normal condition use level 2 access means to enter detection test mode (8.3.8).	Apply at least 5 intruder signals or messages as specified in 8.9. Record the identity of the alarm points activated.	The CIE shall provide means to confirm that each of the activations has been detected.
If the CIE includes "soak test" function (8.3.9)			
2	Use level 3 access means to place at least 2 alarm points on soak test.	Record alarm points so programmed and, where removal is automatic, time period for test.	
3	Set the CIE.	Record indications during the setting procedure.	During the setting procedure, an indication shall be provided that alarm points are being soak tested, in accordance with 8.3.9.
4	Whilst CIE is set, activate the alarm points that are being tested.	Record the identity of the alarm points activated and the condition of indication and notification outputs of the CIE.	The activations shall not be notified.
5	Unset the CIE.	Record the condition of indication outputs and event logs.	The activations shall be indicated at the time of unsetting in accordance with 8.5. Logging shall be in accordance with 8.3.9 and 8.10.
6	Where removal from test mode is automatic:	Repeat steps 3 and 4 one day before test period is due to end.	Test shall remain active.
7		Repeat steps 3 and 4 after test period is due to expire.	There shall be no indication at step 3 and an alarm shall be notified and indicated at step 4.
8	Where removal from test mode is not automatic:	Use level 3 access means to remove the alarm points from soak test.	

11.7.8 Other functions

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to function normally whilst a non-IEC 62642-1 function is used, as required by 8.3.10.

b) Principle

The test consists of operating an additional function during a normal CIE operation and verifying that compliance with this standard is not affected.

The manufacturer shall advise on what additional functions are provided and how these may be operated which I&HAS functions the additional function may interfere with.

c) Test condition

The CIE shall be in the condition appropriate to testing the I&HAS function identified.

d) Procedure

Operate the I&HAS and additional functions simultaneously (or within an agreed time).

e) Measurement

Monitor the operation of the I&HAS function.

f) Pass/fail criteria

The operation of the I&HAS function shall comply with the requirements of this standard.

11.7.9 Monitoring of CIE processing

a) Object of the test

The object of the test is to demonstrate the ability of the CIE with programme controlled serial data processing to comply with 8.4.3 to detect and react to processing faults.

b) Principle

The test consists of introducing a fault in the processing and monitoring that the correct indication(s) and notification(s) occur, see Table 29.

The manufacturer shall advise on how a processing failure may be induced for test purposes.

Table 29 – Test of CIE process monitoring

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	The CIE shall be in the unset mode, with all inputs and outputs in normal condition.	Induce a failure of the processing function.	Record the status of process monitoring output.	In grade 3 and 4 the output shall change status within 40 s unless the CIE has successfully restarted sooner.
2		Remove failure mode and apply the reduced functional test.	Record the status of the CIE, the event log and the indications.	In grades 3 and 4, if the attempt to restart the processor is successful, the CIE shall resume in its previous operating mode, the reduced functional test shall be completed successfully and a CIE fault shall be indicated and recorded in the event log.

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
3	Repeat steps 1 & 2 as above for “set mode”.	Repeat as above.	As above.	As above.

11.7.10 Availability of indications

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with the requirements of 8.5.1.

b) Principle

The test consists of introducing a condition requiring a mandatory indication and ensuring that the requirements of IEC 62642-1, 8.5.2 and 8.5.3 are met, in accordance with Table 30.

Table 30 – Test of availability of indications

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	The CIE shall be in the unset mode, with all inputs and outputs in normal condition.	Induce a fault requiring mandatory indication according to IEC 62642-1, Table 8.	Record indications.	Alert indication present
2	Gain access to CIE at level 2.	View information displayed.	Record indications.	Correctly indicates fault condition generated.
3	Return to level 1 access in accordance with manufacturer’s specification – using automatic (timed) response if provided.	View information displayed.	Record indications.	Alert indication present If automatic (timed) action, it is performed within time limit specified by manufacturer.
4	Remove the fault condition applied at step 1.	View information displayed.	Record indications.	Alert indication present
5	Gain access to CIE at level 2.	View information displayed.	Record indications.	Indication of the fault condition remains available.
6	Return to access level 1 and restore.	View information displayed.	Record indications.	No indication

11.8 Tamper security tests

11.8.1 ACE type A

Documentation provided by the manufacturer to justify a claim of “type A” status for ACE shall be verified.

11.8.2 Tamper protection

a) Principle

The principle of this test is to use impact testing to verify that the CIE/ACE housing meets the tamper protection requirements of 8.7.1.

b) Procedure

Subject the CIE/ACE housings to impact testing using the methodology of IEC 62599-1, with equipment meeting the requirements of IEC 60068-2-75:1997 at the severity levels specified in 8.7.1.

c) Measurement

Assess the EUT as described in the reduced functional test in 11.3.

d) Pass/fail criteria

The EUT shall meet the requirements of the reduced functional test before, during and after the test.

The generation of signals or messages is permitted as a result of this test.

There shall be no signs of mechanical damage that will permit access to internal elements of the CIE/ACE housing unless a tamper signal or message has been generated.

There shall be no damage to the ACE housing that would permit the status of the I&HAS to be changed or prevent the CIE from initiating all mandatory notification responses.

11.8.3 Tamper detection – Access to the inside of the housing

a) Principle

The principle of this test is to verify that it is not possible to insert a tool into the CIE/ACE in its normal mounting position and defeat the operation of the tamper detection circuitry before a tamper signal or message is generated (see 8.7.2.1).

b) Test conditions

The CIE should be in unset condition.

c) Mounting

Mount the CIE/ACE according to the manufacturer's instructions with the housing securely closed.

d) Procedure

Open the CIE/ACE housing by normal means and attempt to introduce a sabotage tool as specified in 8.7.2.1, into the EUT without causing physical damage before the tamper detection device operates.

NOTE The tool may be inserted through any aperture, before or during the process of opening the housing. For grades 3 and 4, this includes apertures for indicators and operating controls that are accessible to a level 1 user.

If the tool is successfully inserted, it should be manoeuvred to try to interfere with the tamper detection device. The wire test includes forming the wire as appropriate.

Attempts shall be restricted to 5 min per tool (10 min for grade 4). If the test fails, it should be repeated and a further failure within 4 further attempts shall result in the overall test failing.

e) Measurement

Record the generation of the tamper signal or message.

f) Pass/fail criteria

Opening the CIE/ACE by normal means shall only be possible by following the procedure defined by the manufacturer and shall generate a tamper signal or message.

a) either, the tamper detection device shall not have been defeated before the generation of a tamper signal or message,

b) or visible damage has been caused in order to defeat the tamper detection device.

11.8.4 Tamper detection – Removal from mounting

a) Principle

The principle of this test consists of removing the CIE/ACE from its mounting surface and monitoring the EUT to determine whether a tamper signal or message is generated within the required time period when the maximum permitted distance (see 8.7.2.2) is exceeded.

b) Test conditions

The CIE should be in the unset condition.

c) Mounting

Position the EUT on a horizontal flat surface, taking into account any requirements specified by the manufacturer to operate the removal from mounting detection device.

d) Procedure

Lift the EUT from the flat surface in a perpendicular direction to the mounting surface by a distance exceeding that specified in 8.7.2.2, whilst monitoring the tamper signal or message output.

Attempt to slide a test blade as defined in 8.7.2.2 to defeat the removal from mounting detection before and during the above test.

Attempt to use pliers as specified in 8.7.2.2 to defeat the removal from mounting detection before and during the above test.

Attempts shall be restricted to 5 min per tool (10 min for grade 4). If the test fails, it should be repeated and a further failure within 4 further attempts shall result in the overall test failing.

e) Measurement

Monitor the tamper signal or message output.

Record whether it was possible to prevent the generation of a tamper signal or message using the test blade or pliers.

f) Pass/fail criteria

The tamper signal or message shall have been generated within 11 s of the EUT exceeding the distance specified in 8.7.2.2.

It shall not have been possible to prevent the generation of a tamper signal or message using the test blade or pliers.

11.8.5 Tamper detection – Penetration of the housing

a) Principle

The principle of this test consists of drilling a hole in an accessible face of the housing and verifying that a tamper signal or message is generated (see 8.7.2.3).

b) Test conditions

The I&HAS should be in the unset condition.

c) Mounting

Mount the EUT according to the manufacturer's instructions with the housing securely closed.

d) Procedure

Drill a hole of 4 mm diameter in any accessible face of the EUT using a metal drill bit.

e) Measurement

Monitor the tamper signal or message output.

f) Pass/fail criteria

A tamper signal or message shall be generated when a hole of 4 mm is made in any accessible face of the housing.

11.9 Substitution tests

11.9.1 Tests for monitoring of substitution of components

The manufacturer shall provide information from which it can be verified that the method of monitoring is compliant with the requirement of IEC 62642-1, 8.7.3.

11.9.2 Tests for monitoring of substitution – Timing requirements

The manufacturer shall provide information from which it can be verified that the method of monitoring is compliant with the timings requirement specified in IEC 62642-1, 8.7.4.

11.10 Testing of I&HAS timing performance

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.9 and the timing requirement of IEC 62642-1, 8.8.1.

b) Principle

The test consists of introducing a notifiable event and ensuring that this takes place within the time specified by IEC 62642-1, 8.8.1 and 8.9.1.

c) Procedure

With the system in set mode, trigger an intruder alarm event.

d) Measurement

Record the time before the notification output(s) become live.

e) Pass/fail criteria

The time from triggering the event until notification takes place shall not exceed 20 s.

For message structured systems:

- the manufacturer shall provide information to enable the time at which the message originated to be determined;
- the manufacturer shall provide evidence that this timing requirement can be maintained under the slowest possible communication conditions in an installed system.

11.11 Testing for interconnections

11.11.1 Monitoring of interconnections

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.8 and the timing requirement of IEC 62642-1, 8.8.3.

b) Principle

The test consists of simulating the interconnection being disabled and monitoring the response.

NOTE The manufacturer may need to provide details of how this may be done.

c) Procedure

a) Disable the interconnection (for example: by short circuit).
b) If the system uses non-specific interconnections, simulate another application taking permanent control of the interconnection.

d) Measurement

Record the system response and measure the time taken for the system to respond.

e) Pass/fail criteria

In each case, the response shall comply with the requirements of IEC 62642-1, 8.8.3.

11.11.2 Testing of monitoring of periodic communication

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.8 and the timing requirement of IEC 62642-1, 8.8.4.1.

b) Principle

The manufacturer shall provide means to, either

a) verify from documentation that the system response would comply with the requirements of IEC 62642-1, Table 17,

or

b) identify the point at which a periodic communication takes place in order to test as follows.

c) Procedure

With the system in set mode, apply a fault condition (for example: short circuit) to the interconnect, immediately following the identified periodic communication.

d) Measurement

Measure time for system to respond.

e) Pass/fail criteria

System response defined by IEC 62642-1, Table 20 shall occur within the time specified by IEC 62642-1, Table 17.

11.11.3 Testing of verification during setting procedure

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to comply with 8.8 and the timing requirement of IEC 62642-1, 8.8.4.2.

b) Principle

The manufacturer shall provide means to, either

a) verify from documentation that the system response would comply with the requirements of IEC 62642-1, Table 18,

or

b) identify the point at which a periodic communication takes place in order to test as follows.

c) Procedure

With the system in unset mode, apply a fault condition (example: short circuit) to the interconnect, immediately following the identified periodic communication for the period required by Table 18. Attempt to set the I&HAS.

d) Measurement

Monitor the status of the I&HAS.

e) Pass/fail criteria

The I&HAS shall not set.

11.11.4 Test for security of communication

The manufacturer shall provide information from which compliance with the requirements of IEC 62642-1, 8.8.5 can be verified.

11.12 Event log

a) Object of the test

The object of the test is to demonstrate the ability of the CIE to maintain an event log and keep an accurate clock in accordance with the requirements of 8.10.

b) Principle

The test consists of operating the CIE to ensure correct operation of the event log, whilst ensuring the long-term accuracy of the clock (see Table 31).

c) Test condition

The test shall be run with the system initially in the unset condition.

Table 31 – Test of event log

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	With the CIE unset and with no alarm condition, set the time and date.	Note the date and time.	
2	With the system unset and in the normal condition enter an authorisation code at each access level.	Note the facilities accessible to each access level.	There shall be no facility for a user to alter or delete the event log.
3	If the means of recording is cyclic: Fill the event log. With the system unset, add one more mandatory event.	Note the 2 oldest events before the final event is added. Note the oldest event after the final event is added.	The oldest event shall be deleted by the last added mandatory events.
4	If the CIE has the facility to record non-mandatory events, then enter the appropriate number of mandatory events as defined in IEC 62642-1, 8.10. Fill the remainder of the event log with non-mandatory events. Add one non-mandatory event.	Note the mandatory events recorded in the event log.	Verify that minimum permitted number of mandatory events has been preserved.
5	Following the previous test (C), add one mandatory event.	Note the mandatory events recorded in the event log.	Verify that the new mandatory event has been logged.
6	If memory retention component(s) are non-volatile (example; EEPROM): Check data supplied by manufacturer.		Verify that storage component(s) are non-volatile for the period required by IEC 62642-1, Table 21.
7	If memory retention components are volatile (example; RAM): Remove EPS and APS from the system for the period required by IEC 62642-1, Table 21. At the end of this period, reapply power and check the event log.	Record the contents of the event log before removal of power and after power is restored.	The contents of the event log shall not be lost or corrupted, except for the inclusion of event(s) caused by this test procedure (for example: mains failure)

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
8	In CIE with the facility to make a permanent record, follow manufacturer's instructions to make a permanent record.	Note the event log and the events recorded on the permanent record.	The events displayed on the permanent record shall accurately reflect the event log, including date and time.
9	Checking the clock accuracy.	When the system has been running for a minimum 8 day period note the indicated time by the CIE.	The accuracy shall be consistent with IEC 62642-1, 8.10.
Where the I&HAS stores event logs at the ARC, the manufacturer shall provide information or means to enable this function to be tested as follows:			
10	Check ability of CIE to send events to the SPT. Generate an event at the CIE.	Monitor the output to the SPT.	Verify that the generated events are sent to the SPT.
11	Check ability of CIE to indicate failure of transmission to the ARC: Disable the SPT and generate a number of mandatory events in accordance with IEC 62642-1, 8.10, to be reported to the ARC.	Record the indication and notification at the CIE.	Verify that a fault is indicated at the CIE (grade 1).
12	Enable the SPT.		For CIE grades 2, 3 and 4, the event(s) shall be transmitted when the SPT is re-enabled.

11.13 Marking and documentation

a) Principle

The principle of this test is to verify that the marking of the CIE and the documentation supplied with the CIE meet the requirements of Clauses 9 and 10.

b) Procedure

Examine the marking of the CIE and ACE.

Examine the documentation supplied by the CIE manufacturer.

c) Pass/fail criteria

The marking on the CIE and ACE shall meet the requirements of Clause 10 of this standard.

The documentation shall meet the requirements of Clause 9 of this standard.

NOTE Durability tests of labelling are carried out as part of the low voltage regional directive testing.

11.14 Environmental and EMC tests

The environmental classification is described in IEC 62642-1. Relevant environmental tests carried out shall be in accordance with IEC 62599-1.

Where the reduced functional test is specified during the environmental and EMC conditioning, this shall be carried out as detailed in IEC 62599-1.

For operational tests, CIE and ACE shall not generate alarm, tamper, fault or other signals or messages or change from one mode to another, when subjected to the specified range of environmental and EMC conditions and shall continue to function normally.

For endurance tests, the CIE and ACE shall pass the reduced functional test after being subjected to the specified range of environmental conditions.

See Table 32 for the relevant tests for each environmental class. These tests apply to all security grades.

Table 32 – Environmental and EMC tests

	Reduced functional test (11.3)	Test	Type	Class I	Class II	Class III	Class IV
1	B, D, A	Dry heat	Operational	M	M	M	M
2	B, A	Dry heat	Endurance	N/A	N/A	N/A	M
3	B, D, A	Cold	Operational	M	M	M	M
4	B, D, A	Damp heat, steady state	Operational	M	N/A	N/A	N/A
5	B, A	Damp heat, steady state	Endurance	M	M	M	M
6	B, D, A	Temperature change (p)	Operational	M	M	M	M
7	B, D, A	Damp heat, cyclic	Operational	N/A	M	M	M
8	B, A	Damp heat, cyclic	Endurance	N/A	N/A	M	M
9	B, C, A	Water ingress	Operational	M (p)	M (p)	M	M
10	B, A	Sulphur dioxide (SO_2)	Endurance	N/A	N/A	M	M
11	B, A	Salt mist, cyclic	Endurance	N/A	N/A	N/A	M
12	B, C, A	Impact (f) (m)	Operational	M	M	M	M
13	B, C, A	Free fall (m) (p)	Operational	M	M	M	M
14	B, C, A	Shock (f)	Operational	M	M	M	M
15	B, C, A	Vibration, sinusoidal	Operational	M	M	M	M
16	B, C, A	EMC tests	Operational	M	M	M	M

Key

A After conditioning and recovery period.

B Before conditioning.

C Monitor during conditioning with CIE in set mode.

D During conditioning, monitor with CIE in set mode and conduct reduced functional test when specified in IEC 62599-1.

M Mandatory.

N/A Not applicable.

(f) Applicable to fixed equipment.

(m) Applicable to moveable equipment.

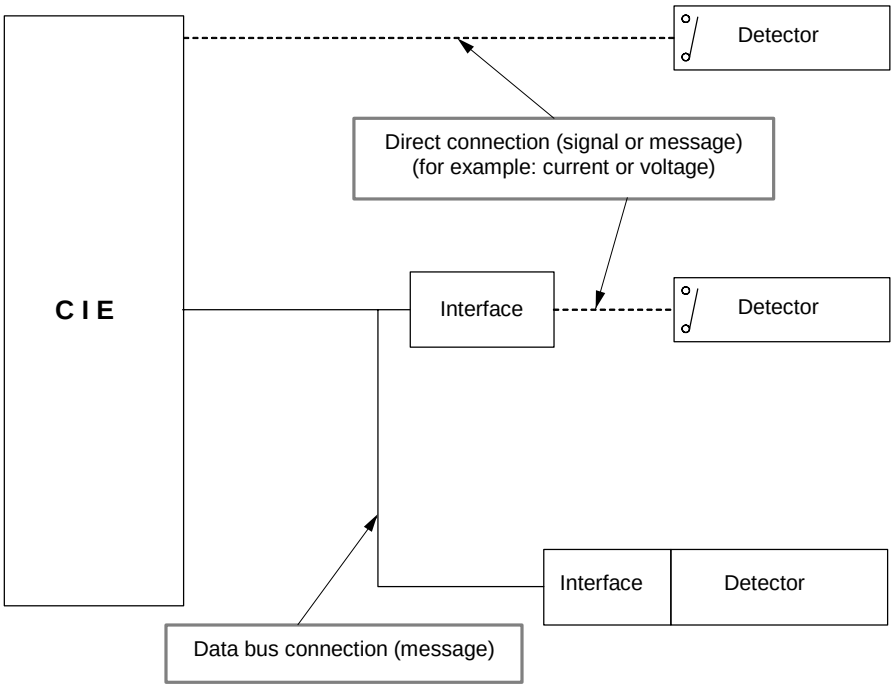
(p) Applicable to portable equipment.

Annex A
(informative)

Interconnection types

This annex is intended to clarify terms defined in IEC 62642-1, Clause 3.

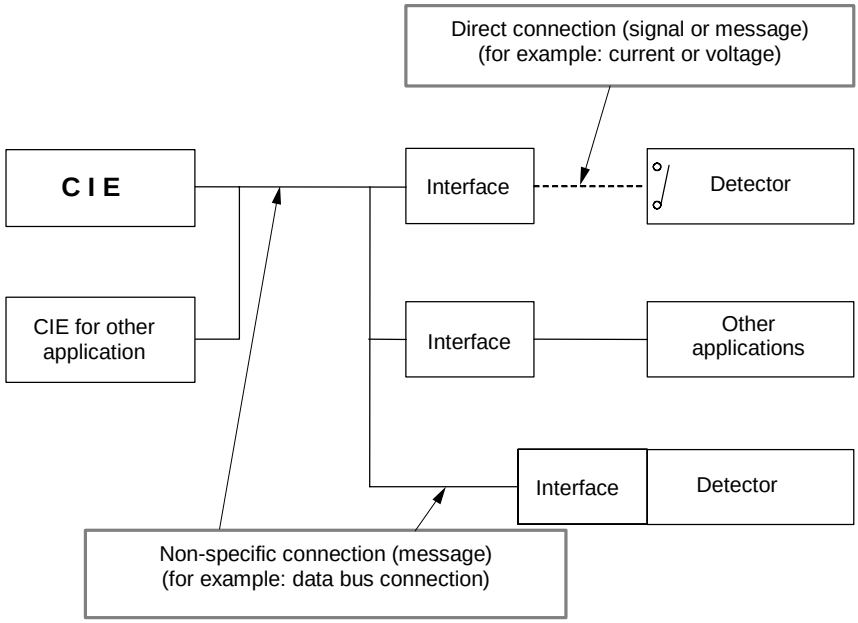
A.1 Specific wired interconnections



NOTE Interfaces may take any relevant form (for example: expansion, device capable of accepting inputs from a number of detectors, module to interface a single detector, etc.).

Figure A.1 – Specific wired interconnections

A.2 Non-specific wired interconnections



NOTE Interfaces may take any relevant form (for example: expansion, device capable of accepting inputs from a number of detectors, module to interface a single detector, etc.).

Figure A.2 – Non-specific wired interconnections

A.3 Wire-free interconnections

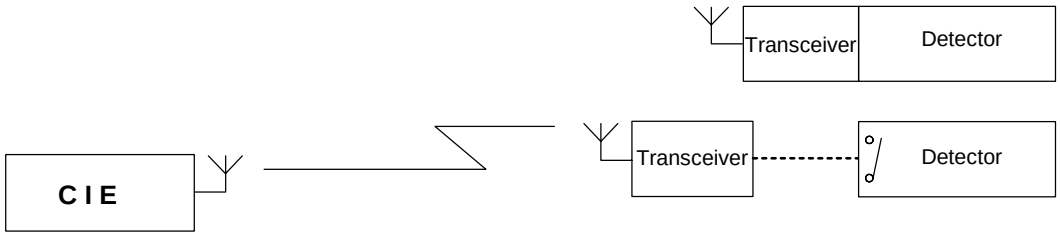


Figure A.3 – Wire-free interconnections

Wire-free interconnections shall comply with the requirements of IEC 62642-5-3.

A.4 Signals – Active period

When a direct connection is used between the CIE and a detector and alarm information is sent as an electrical signal, then the active period of the signal is the period for which the detector output relay (or magnetic contact or electrically driven current or voltage) is in the alarm condition.

Annex B
(informative)

Summary of timing requirements

Table B.1 – Timing table

	Reference	Process if more than	Process and notify within	Minimum	Maximum
Intruder signal	8.9	400 ms	10 s		
Hold-up signal	8.9	400 ms	10 s		
Tamper signal	8.9	400 ms	10 s		
Fault signal	8.9	10 s	10 s		
Masking signal – processed as intrusion	8.9 / IEC 62642-1, 8.4.5	400 ms	10 s		
Masking signal – processed as fault	8.9 / IEC 62642-1, 8.4.5	10 s	10 s		
Significant reduction of range signal – processed as intrusion	8.9 / IEC 62642-1, 8.4.6	400 ms	10 s		
Significant reduction of range – processed as fault	8.9 / IEC 62642-1, 8.4.6	10 s	10 s		
WD activation delay after remote notification	8.6			0	10 min
WD duration	8.6			90 s	15 min
EPS fault	8.6	10 s	1 h [a]		
Main program watchdog	8.4.3	10 s	30 s [a]		
Duration of the “set indication” after SET	8.3.3				[b]
Duration of the “unset indication” after UNSET	8.3.4				30 s
Unsetting procedure duration	8.3.4				45 s

[a] May be cancelled if condition restores during this delay period.

[b] This indication is specified as “time limited” – but no actual limit is specified in IEC 62642-1. The time limit does not apply to grade 1 and 2 systems using IEC 62642-1, 8.3.7, option c).

Annex C
(normative)

Use of non-I&HAS interface

A degree of control of the I&HAS may be duplicated by a device not part of the I&HAS (for example: a computer or PDA). The CIE may provide a logical gateway for the connection of such a device, which may be connected by any suitable means, be fixed or portable and be located in or remotely from the supervised premises.

The communications software protocols shall ensure that substitution, message security and authorisation integrity comply with the requirements of Table C.1.

The control device may be configured to operate with more than one I&HAS or other system(s).

All system actions initiated from the non-I&HAS interface shall be uniquely identifiable in the CIE event log.

Because of the nature of the connections and protocols used, some I&HAS system requirements are inappropriate (e.g. secure software protocols to replace the need for tamper protection) and therefore the following modified conditions shall apply to the non-I&HAS interface and connections thereto:

Table C.1 – Conditions for use of non-I&HAS interface for control and indicating purposes

IEC 62642-3	Function	Expected behaviour
7	Environmental requirements	Not applicable
8.3.2	Authorisation	Access to the communications software at the non-I&HAS interface shall comply with this requirement.
	Authentication	Initiation of communication between the non-I&HAS interface and the I&HAS shall have authentication equivalent to the requirements of 8.3.2.
8.5.1	Indications	Indications at the non-I&HAS interface may be considered as equivalent to a mimic panel (see 8.5.1, NOTE 3).
8.7.1	Tamper protection	Not applicable
8.7.2	Tamper detection	Not applicable
8.7.3	Monitoring of substitution	The requirement shall apply at all grades. [a]
8.7.3	Timing requirements	The grade 3 requirement shall apply additionally at grades 1 and 2. [a]
8.8	Monitoring of interconnections	The requirement of IEC 62642-1, 8.8.3 (Table 16) is not applicable to portable devices.
8.8	Security of communication	The requirement of IEC 62642-1, 8.8.5 (Table 19) shall apply at all grades.
8.11	Power supply	The requirement of IEC 62642-1, 9.2 for APS is not applicable.
[a] If the device does not include the capability to provide input to the I&HAS, this requirement is not applicable.		

Annex D
(informative)

Summary of function cross-references

Table D.1 – Cross-references

IEC 62642-1	IEC 62642-3	Function	Grade					Test(s)
			1	2	3	4		
8.1	-	Detection						-
	8.1	Inputs						-
8.1.1	8.1.1	Intruder detection	M	M	M	M		11.4.1
8.1.2	8.1.2	Hold-up device triggering	Op	Op	Op	Op		11.4.2
8.1.3	8.1.3	Tamper detection	M	M	M	M		11.4.3
8.1.4 (T.1)	8.1.4	Recognition of faults	M	M	M	M		11.4.4
	8.1.5	User	M	M	M	M		11.5.1
8.2.1	8.1.6	Masking	Op	Op	M	M		11.4.5
8.2.2	8.1.7	Detector range reduction	Op	Op	Op	M		11.4.6
	8.1.8	Other inputs	Op	Op	Op	Op		11.4.7
	8.2	Outputs	Op	Op	Op	Op		-
8.3	8.1.5 / 8.3 /8.4.2	Operation (controls)	M	M	M	M		11.5.1
8.3.1 (T.2)	8.3.1	Levels of access	M	M	M	M		11.5.1
8.3.2 (T.3)	8.3.2	Authorization	M	M	M	M		-
	8.3.2.1	Mechanical keys	Op	Op	Op	Op	Shall include at least one of these	11.6.1
	8.3.2.2	Logical keys	Op	Op	Op	Op		11.6.2
	8.3.2.2.1	PIN codes	Op	Op	Op	Op		11.6.2.2
	8.3.2.2.2	Digital keys	Op	Op	Op	Op		11.6.2.1
	8.3.2.2.3	Biometric keys	Op	Op	Op	Op		11.6.2.3
	8.3.2.3	Combinations of keys	Op	Op	Op	Op		11.6.2.4
	8.3.2.4	Repeated invalid codes	Op	M	M	M		11.6.3
8.3.3	8.3.3 / 8.3.4	Setting/Unsetting	M	M	M	M		11.7.1 – 11.7.5
8.3.4	8.3.3	Setting	M	M	M	M		11.7.1, 11.7.5
8.3.5 (T.4)	8.3.3.1	Prevention of setting	M	M	M	M		11.7.2
8.3.6 (T.5)	8.3.3.1	Override prevention of setting	Op	Op	Op	Op		11.7.2; 11.7.5
	8.3.3.2	Exit route facility	Op	Op	Op	Op		11.7.1
	8.3.3.3	Fail to set	M	M	M	M		11.7.1
8.3.7	8.3.3.4	Set state	M	M	M	M		11.7.3
8.3.8.1	8.3.4	Unsetting	M	M	M	M		11.7.4; 11.7.5
8.3.8.2	8.3.4	Unsetting as in IEC 62642-1 - 8.3.7 b) (with entry route)	Op	Op	Op	Op		11.7.4
8.3.9 (T.6)	8.3.5	Restoring	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1

IEC 62642-1	IEC 62642-3	Function	Grade					Test(s)
			1	2	3	4		
8.3.10	8.3.6	Inhibit	Op	Op	Op	Op		11.5.1; 11.7.1; 11.7.6
-	8.3.6.1	Automatic inhibit	Op	Op	Op	Op		-
8.3.11	8.3.7	Isolate	Op	Op	Op	Op		11.5.1; 11.7.6
8.3.12	8.3.8	Level 2 user test	M	M	M	M		11.7.7
-	8.3.9	Soak test	Op	Op	Op	Op		11.7.7
8.3.13	8.3.10	Other functions	Op	Op	Op	Op		11.7.8
8.4 (T.7)	8.4	Processing	M	M	M	M		11.4.1
8.4.1	8.4.1 8.4.1.1	Intruder signals/messages	M	M	M	M		11.4.1
8.4.2	8.4.1	Hold-up signals/messages	Op	Op	Op	Op		11.4.2
8.4.3	8.4.1	Tamper signals/messages	M	M	M	M		11.4.3
8.4.4	8.4.1	Fault signals/messages	M	M	M	M		11.4.4
8.4.5	8.4.1	Masking signals/messages	Op	Op	M	M		11.4.5
8.4.6	8.4.1	Reduction of range signals/messages	Op	Op	Op	M		11.4.6
	8.4.1.2	Priorities	M	M	M	M		11.4.1
	8.4.2	User input	M	M	M	M		11.5.1
	8.4.3	Monitoring of CIE processing	Op	Op	M	M		11.7.9
8.5.1 (T.8)	8.5.1	Indications – general	M	M	M	M		11.4.1/2/3/4/5/6
8.5.2 (T.9)	8.5.1 and 8.5.1.1	Availability of indications	M	M	M	M		11.4.1/2/3/4/5/6 11.7.10
	8.5.1.2	Other indications	Op	Op	Op	Op		11.4.7
8.5.3	8.5.1	Cancelling of indications	M	M	M	M		11.4.1/2/3/4/5/6 11.7.10
	8.5.2	Visual indications	M	M	M	M		-
	8.5.3	Priorities	M	M	M	M		-
8.5.4	-	Indication – intrusion detectors	-	-	-	-		-
8.6 (T.10 and T.11)	8.6	Notification	M	M	M	M		11.4.1/2/3/4/5/6
8.7.1	8.7.1	Tamper protection	M	M	M	M		11.8.2
8.7.2 (T.12 and T.13)	8.7.2	Tamper detection						
	8.7.2.1	Opening of housing	M	M	M	M		11.8.3
	8.7.2.2	Removal from mounting	Op	Op	M	M		11.8.4
	8.7.2.3	Penetration of housing	Op	Op	Op	M		11.8.5
8.7.3 (T.14)	8.7.3	Monitoring of substitution	Op	Op	Op	M		11.9
8.7.4 (T.15)	8.7.3	Substitution - timing	Op	Op	Op	M		11.9
8.8.1	8.8	Interconnections – general	M	M	M	M		11.10
8.8.2	8.8	Interconnections – availability	M	M	M	M		11.11

IEC 62642-1	IEC 62642-3	Function	Grade					Test(s)
			1	2	3	4		
8.8.3 (T.16)	8.8	Interconnections – monitoring	M	M	M	M		11.11
8.8.4.1 (T.17)	8.8	Verification – periodic communication	M	M	M	M		11.11
8.8.4.2 (T.18)	8.8	Verification – during set period	M	M	M	M		11.11
8.8.5 (T.19)	8.8	Security of communication	Op	Op	Op	M		11.11
8.8.6 (T.20)	8.8	Signals/messages generated (IEC 62642-1 Sublauses 8.8.3 / 8.8.4 / 8.8.5)	M	M	M	M		11.11
8.9.1	8.9	Timing – intruder, tamper, faults	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
8.9.2	8.9	Processing	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
8.10 (T.21 and T.22)	8.10	Event recording	Op	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
	8.10.1	Event recording at CIE	Op	M	M	M		11.12
	8.10.2	Event recording at ARC	Op	Op	Op	Op		11.12
9.1	-	Types of PS	-	-	-	-		-
9.2 (T.24)	-	PS requirements	-	-	-	-		-
	8.11	Power supply	M	M	M	M		EN 50131-6
10	-	Operational reliability	M	M	M	M		-
11	-	Functional reliability	M	M	M	M		-
12	7	Environmental requirements	M	M	M	M		11.14
12.2	-	Electromagnetic Compatibility	M	M	M	M		11.14 and EMCD
13	-	Electrical safety	M	M	M	M		LVD
14.1	-	I&HAS documentation						
14.2	9	Product documentation	M	M	M	M		11.13
15	10	Marking/identification	M	M	M	M		11.13

M = Mandatory

Op = Optional

NOTE All I&HAS functions provided and claimed by the manufacturer should be tested (see 4.1).

Bibliography

IEC 62262, *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)*

IEC 62642-2 (all parts), *Alarm systems – Intrusion and hold-up systems – Part 2: Intrusion detectors*

EN 50136 (all parts), *Alarm systems – Alarm transmission systems and equipment*

CLC/TS 50398, *Alarm systems – Combined and integrated alarm systems – General requirements*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES D'ALARME – SYSTÈMES D'ALARME CONTRE L'INTRUSION ET LES HOLD-UP –

Partie 3: Equipement de contrôle et de signalisation

AVANT-PROPOS

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

La Norme internationale CEI 62642-3 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme et de sécurité électroniques.

La présente norme est basée sur l'EN 50131-3 (2006).

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/310/FDIS	79/321/RVD

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

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

Une liste de toutes les parties de la série CEI 62642, présentées sous le titre général *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up,* peut être consultée sur le site web de la CEI.

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

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

INTRODUCTION

La présente partie 3 de la série de normes CEI 62642 donne les exigences pour les équipements de contrôle et de signalisation utilisés dans les systèmes d'alarme contre l'intrusion et les hold-up. Les autres parties de cette série de normes sont les suivantes:

Partie 1	Exigences système
Partie 2-2	Détecteurs d'intrusion – Détecteurs à infrarouges passifs
Partie 2-3	Détecteurs d'intrusion – Détecteurs à hyperfréquences
Partie 2-4	Détecteurs d'intrusion – Détecteurs combinés à infrarouges passifs et à hyperfréquences
Partie 2-5	Détecteurs d'intrusion – Détecteurs combinés à infrarouges passifs et à ultrasons
Partie 2-6	Détecteurs d'intrusion – Détecteurs d'ouverture à contacts (magnétiques)
Partie 2-71	Détecteurs d'intrusion – Détecteurs de bris de verre – Acoustiques
Partie 2-72	Détecteurs d'intrusion – Détecteurs de bris de verre – Passifs
Partie 2-73	Détecteurs d'intrusion – Détecteurs de bris de verre – Actifs
Partie 3	Equipement de contrôle et de signalisation
Partie 4	Dispositifs d'avertissement
Partie 5-3	Interconnexions – Exigences pour les équipements utilisant des techniques radio fréquence
Partie 6	Alimentation
Partie 7	Guide d'application
Partie 8	Systèmes/dispositifs générateurs de fumée

Afin d'assurer la cohérence de l'ensemble des documents de la série CEI 62642, la terminologie est définie à un seul endroit qui est le document maître CEI 62642-1 et qui décrit les exigences générales concernant le système d'intrusion. Des exceptions sont faites pour des termes spécifiques aux organes de contrôle et d'indication et là où leur répétition est considérée comme essentielle pour la clarté du document.

Une référence aux diverses implications découlant des normes relatives aux détecteurs a été incluse. L'ensemble des détails relatifs aux exigences en matière d'interconnexion peut faire l'objet d'une future norme.

Un certain nombre d'exigences sont contenues dans la présente norme pour laquelle une procédure formelle d'essai ne peut être rédigée qu'en définissant (et donc en restreignant) la technologie au moyen de laquelle l'exigence est satisfaite. En conséquence, il a été reconnu que ces fonctions ne peuvent être soumises à un essai que par un accord entre le fabricant et le laboratoire d'essai selon des informations documentées relatives au mode de satisfaction de la fonctionnalité requise.

Un tableau des références croisées correspondant aux exigences contenues dans la CEI 62642-1 et à la présente norme et à ses essais est inclus en Annexe D.

SYSTÈMES D'ALARME – SYSTÈMES D'ALARME CONTRE L'INTRUSION ET LES HOLD-UP –

Partie 3: Equipement de contrôle et de signalisation

1 Domaine d'application

La présente partie de la CEI 62642 spécifie les exigences, critères de performance et procédures d'essai pour les équipements de contrôle et de signalisation (centrales d'alarme) (CIE) destinés à être utilisés dans les systèmes d'alarme contre l'intrusion (IAS) et les systèmes d'alarme contre les hold-up (HAS) installés dans les bâtiments. Le présent document s'applique également aux CIE destinés à être utilisés dans les systèmes IAS ou HAS.

Les CIE peuvent incorporer des fonctions de traitement d'autres composants IAS et HAS ou leurs exigences de traitement peuvent être réparties entre ces composants.

La présente norme spécifie les exigences relatives aux CIE installés dans des bâtiments qui utilisent des liaisons filaires spécifiques ou non spécifiques ou des liaisons sans fil. Ces exigences s'appliquent également aux matériels de commande auxiliaire (ACE) installés à l'intérieur ou à l'extérieur des bâtiments surveillés et montés dans un environnement intérieur ou extérieur.

Lorsque le CIE partage des moyens de détection, d'interconnexion, de commande, de communication, de traitement et/ou des alimentations avec d'autres applications, ces exigences ne s'appliquent qu'aux fonctions IAS et HAS.

La présente norme spécifie les exigences de performance pour les CIE pour chacun des quatre grades de sécurité identifiés dans la CEI 62642-1. Des exigences sont également spécifiées pour quatre classes d'environnement couvrant des applications pour des emplacements intérieurs et extérieurs.

La présente norme inclut des fonctions obligatoires, qui doivent être assurées pour tous les CIE pour le grade approprié de sécurité, ainsi que des fonctions facultatives complémentaires.

NOTE Dans la présente norme, il est fait référence au terme "I&HAS" dans l'intégralité de celle-ci sauf lorsqu'il est spécifiquement nécessaire de différencier les parties IAS et HAS d'un système. Le terme est destiné à inclure IAS et HAS lorsque ces systèmes sont installés séparément.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence (y compris les éventuels amendements) s'applique.

CEI 60068-1:1988, *Essais d'environnement – Partie 1: Généralités et guide*

CEI 60068-2-75:1997, *Essais d'environnement – Partie 2-75: Essais – Essai Eh: Essais aux marteaux*

CEI 60073, *Principes fondamentaux et de sécurité pour l'interface homme-machine, le marquage et l'identification – Principes de codage pour les indicateurs et les organes de commande*

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

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

CEI 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*

CEI 62642-1:2010, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 1: Exigences système*

CEI 62642-5-3, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 5-3: Interconnexions – Exigences pour les équipements utilisant des techniques radio fréquence*

EN 50131-6:2008, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 6: Alimentation*[1]

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 62642-1, ainsi que les termes et définitions suivants s'appliquent.

3.1.1
validation
action d'un utilisateur pour accepter une indication

3.1.2
point d'alarme
un ou plusieurs détecteur(s) délivrant un signal ou un message commun, au CIE ou à l'ACE aux fins d'indication ou de traitement

3.1.3
signal ou message d'alarme
signal ou message généré par un point d'alarme

3.1.4
clé biométrique
utilisation d'une caractéristique biométrique par un utilisateur autorisé afin d'avoir accès à des fonctions ou des parties restreintes d'un CIE

EXEMPLE: empreinte digitale ou reconnaissance de l'iris.

3.1.5
conditionnement
exposition de l'équipement soumis à l'essai (EUT) à des conditions d'environnement afin de déterminer l'effet de telles conditions sur l'EUT

3.1.6
détecteur
équipement conçu pour générer un signal ou un message d'alarme en réponse à la détection d'une condition particulière indiquant la présence d'un risque

---

1 La transformation de ce document en CEI 62642-6 est en préparation.

3.1.7
clé numérique
dispositif portable contenant des informations codées numériquement utilisé par un utilisateur autorisé pour avoir accès à des fonctions ou des parties restreintes d'un CIE

EXEMPLE: carte magnétique, jeton électronique ou apparenté.

3.1.8
fonction de première issue
moyen permettant d'ignorer des signaux ou des messages en provenance de détecteurs spécifiés pendant une mise hors service pour une période de temps spécifiée

3.1.9
temporisation d'entrée
temps autorisé pour la procédure de mise hors service lorsqu'un chemin d'accès est utilisé

3.1.10
fonction de dernière issue
moyen permettant d'ignorer des signaux ou des messages en provenance de détecteurs spécifiés pendant la mise en service durant une période spécifiée

3.1.11
alimentation externe
EPS
alimentation externe à l'I&HAS qui peut être non continue

EXEMPLE: alimentation principale.

NOTE Uniquement pour les PS de type A et de type B. L'EPS est obtenue comme décrit dans l'EN 50131-6.

3.1.12
échec à la mise en service

condition, lorsque la procédure de mise en service n'a pas été jusqu'à son terme dans le temps attribué, qui maintient l'I&HAS dans l'état hors service

3.1.13
taux de fausse acceptation
FAR
proportion de transactions de vérification biométrique avec des revendications d'identité fausse qui sont incorrectement acceptées

3.1.14
taux de faux rejet
FRR
proportion de transactions de vérification biométrique avec des revendications d'identité authentique qui sont incorrectement rejetées

3.1.15
interaction
toute opération ou action voulue par l'utilisateur pour commander ou faire varier la fonction de l'I&HAS

3.1.16
intrusion
entrée dans les locaux surveillés par une ou des personnes non autorisées

3.1.17
clé logique
informations logiques utilisées par un utilisateur autorisé pour avoir accès à des fonctions ou parties restreintes d'un CIE

EXEMPLE: code PIN, clé numérique, clé biométrique.

3.1.18
clé mécanique
instrument s'appuyant uniquement sur la forme physique afin de déterminer son caractère unique, utilisé par un utilisateur autorisé afin d'avoir accès à des fonctions ou parties restreintes d'un CIE

3.1.19
interface non-I&HAS
dispositif externe au I&HAS permettant de réaliser certaines ou l'ensemble des fonctions de l'ACE

EXEMPLES: ordinateur, PDA.

3.1.20
mode de fonctionnement
en service, hors service, mise en service et mise hors service constituent les quatre modes de fonctionnement

3.1.21
ouvert par des moyens normaux
ouverture du logement de l'équipement au moyen de la procédure définie par le fabricant

3.1.22
numéro d'identification personnel
code PIN
code utilisé par un utilisateur autorisé afin d'avoir accès à des fonctions ou parties restreintes d'un CIE (par exemple, numérique ou alphanumérique)

3.1.23
inhibition
attribut d'un point d'alarme tel que les signaux ou les messages créant normalement des notifications sont empêchés de le faire, mais continuent à être enregistrés dans le journal d'événements

3.1.24
dispositif de stockage
SD
dispositif qui emmagasine l'énergie

EXEMPLE: une batterie.

3.1.25
émetteur-récepteur des locaux surveillés
SPT
appareil placé dans les locaux surveillés incluant l'interface avec l'I&HAS et l'interface avec le réseau de transmission d'alarme

3.1.26
condition d'essai
condition d'un système d'alarme dans lequel les fonctions normales sont modifiées pour des besoins d'essai

3.1.27
entrée pour l'utilisateur
ordre généré par une action délibérée de l'utilisateur

3.1.28
dispositif d'entrée pour l'utilisateur
dispositif utilisé pour l'entrée pour l'utilisateur

EXEMPLES: ACE, verrou physique avec contacts électriques.

3.2 Abréviations

Pour les besoins du présent document, les abréviations suivantes sont utilisées.

ACE[2] matériel de commande auxiliaire
APS[3] source d'alimentation de secours
ARC[4] centre de réception d'alarme
CIE[5] matériel de commande et d'affichage
EPS[6] alimentation externe
EUT[7] équipement soumis à essai
FAR[8] taux de fausse acceptation
FRR[9] taux de faux rejet
HAS[10] système d'alarme contre les hold-up
IAS[11] système d'alarme contre l'intrusion
I&HAS[12] système d'alarme contre l'intrusion et les hold-up
PDA[13] assistant numérique personnel
PIN[14] code d'identification personnel
PS[15] alimentation
SD[16] dispositif de stockage
SPT[17] émetteur-récepteur des locaux surveillés

_____

2 ACE = *ancillary control equipment.*
3 APS = *alternative power source.*
4 ARC = *alarm receiving centre.*
5 CIE = *control and indicating equipment.*
6 EPS = *external power source.*
7 EUT = *equipment under test.*
8 FAR = *false acceptance rate.*
9 FRR = *false rejection rate.*
10 HAS = *hold-up alarm system.*
11 IAS = *intrusion alarm system.*
12 I&HAS = *intrusion and hold-up alarm system.*
13 PDA = *personal digital assistant.*
14 PIN = *personal identification number.*
15 PS = *power supply.*
16 SD = *storage device.*
17 SPT = *supervised premises transceiver.*

WD[18] dispositif d'avertissement

4 Attributs du système

4.1 Généralités

Le CIE doit comprendre, suivant le cas, les attributs nécessaires à la réception des signaux et/ou messages, le traitement des informations, la notification et l'indication. Les exigences détaillées sont fournies à l'Article 8.

NOTE Si une fonction facultative est assurée pour un grade particulier et si la conformité est demandée, il convient que celle-ci réponde aux exigences applicables pour le grade pour lequel la conformité est demandée (si des exigences sont indiquées). En l'absence de spécification pour la fonction au grade en question, il convient que les exigences pour un grade plus élevé (telles qu'elles sont identifiées par le fabricant) s'appliquent.

La conformité à la présente norme doit être démontrée par une évaluation par rapport aux Articles 4 à 10 et la mise en œuvre des essais de l'Article 11.

L'Annexe D fournit les références croisées entre les exigences de la CEI 62642-1 ainsi que les exigences et les essais de la présente norme.

4.2 Fonctionnalités

Les fonctions complétant les fonctions obligatoires spécifiées dans la présente norme peuvent être incluses dans le I&HAS à condition qu'elles n'aient aucune influence sur le bon fonctionnement des fonctions obligatoires.

Lorsqu'elles sont prévues, ces fonctions supplémentaires ne doivent pas avoir d'incidence sur la conformité aux exigences de la présente norme, à l'exception de celles qu'autorise la CEI 62642-1, 8.3.13.

Le CIE peut inclure des fonctionnalités pour des finalités particulières qui rendraient l'I&HAS non conforme à la CEI 62642-1. La documentation du fabricant doit inclure un avertissement à cet effet.

Si l'utilisation d'une ou de plusieurs fonction(s) ou d'une combinaison de fonctions dans le CIE entraînait la non conformité de l'I&HAS installé avec la CEI 62642-1, ou la conformité de celui-ci à un grade de sécurité plus faible (des exemples sont la ou les fonction(s) réduisant la sécurité de l'I&HAS) le fabricant doit, soit:

a) détailler la ou les configurations conforme(s) à la CEI 62642-1;

soit

b) détailler la ou les fonction(s) ou combinaison de fonctions qui entraînerait la non conformité de l'I&HAS installé avec la CEI 62642-1.

Le fabricant doit consigner le fait qu'il convient de supprimer ou de modifier l'étiquetage de conformité si des configurations non conformes sont sélectionnées.

5 Structure du CIE

Le CIE peut se trouver dans un seul boîtier ou être distribué dans de multiples boîtiers et peut être combiné avec les autres composants de l'I&HAS.

Des dispositions doivent être prises pour permettre une fixation satisfaisante du boîtier sur la surface de montage.

_____

[18] WD = *warning device.*

Des systèmes ne faisant pas partie de l'I&HAS peuvent être utilisés pour réaliser des fonctions de l'ACE (par exemple: ordinateur, PDA) si les conditions spécifiées en Annexe C sont satisfaites.

6 Grade de sécurité

Les CIE et ACE doivent être déclarés conformes à l'un des quatre grades de sécurité (le grade 1 étant le plus faible et le grade 4 le plus fort) et doivent satisfaire à l'ensemble des exigences de ce grade.

Les exigences relatives aux performances du CIE varieront en fonction de son grade. Les essais seront réalisés en accord avec le grade précisé dans la documentation et le marquage du CIE.

7 Performances d'environnement

7.1 Exigences

Le CIE et l'ACE doivent fonctionner correctement dans au moins une des classes d'environnement définies dans la CEI 62642-1.

Lorsque les exigences des quatre classes d'environnement sont inadaptées, du fait de conditions extrêmes rencontrées dans certains lieux géographiques, des conditions nationales spéciales sont indiquées dans la CEI 62642-1, Annexe A.

7.2 Essais d'environnement et essais de compatibilité électromagnétique

La CEI 62599-2 spécifie les essais de susceptibilité électromagnétique applicables aux composants de l'I&HAS. Les conditions de fonctionnement pour ces essais sont spécifiées dans le Tableau 32 de la présente norme.

La CEI 62599-1 décrit les méthodes d'essais d'environnement applicables aux composants de l'I&HAS. Les essais applicables sont spécifiés dans le Tableau 32 de la présente norme.

NOTE D'autres aspects environnementaux, couverts par des Directives réglementaires régionales, n'entrent pas dans le domaine d'application de la présente norme.

8 Exigences fonctionnelles

8.1 Entrées

En fonction du grade du CIE et de l'ACE, des moyens doivent être prévus pour recevoir des signaux ou des messages en provenance de détecteurs, de dispositifs de déclenchement de systèmes d'alarme contre les hold-up ainsi que des informations en provenance des dispositifs d'entrée pour l'utilisateur comme spécifié dans les paragraphes suivants.

NOTE 1 La présente norme ne spécifie pas les détails relatifs aux interconnexions, ni le format de ces signaux ou messages. Des détails relatifs aux moyens possibles de transfert de l'information sont inclus dans quelques normes relatives aux composants de la série CEI 62642.

NOTE 2 L'initialisation de certains composants du système peut demander jusqu'à 180 s avant disponibilité des fonctionnalités normales (par exemple: détecteurs).

8.1.1 Détection d'intrusion

Le CIE doit fournir le moyen de recevoir des signaux ou des messages en provenance de détecteurs d'intrusion.

8.1.2 Dispositif du système d'alarme contre les hold-up

Lorsqu'un CIE fournit des dispositifs de système d'alarme contre les hold-up, des moyens doivent être prévus pour recevoir des signaux ou des messages en provenance de dispositifs du système d'alarme contre les hold-up.

8.1.3 Dispositif du système d'alarme contre la fraude

Le CIE doit fournir le moyen de recevoir des signaux ou des messages d'auto surveillance.

8.1.4 Défaut

En fonction du grade, le CIE doit inclure des moyens permettant de reconnaître les conditions de défaut comme spécifié dans le Tableau 1 de la CEI 62642-1, et en plus les défauts indiqués dans le Tableau 1 ci-dessous.

Tableau 1 – Reconnaissance des conditions de défaut supplémentaires

Défauts	Grade 1	Grade 2	Grade 3	Grade 4
Changement de batterie requis [a]	M	M	M	M
Défaut de sortie d'alimentation [b]	Op	Op	M	M
Suivi du traitement	Op	Op	M	M
M = Obligatoire Op = Facultatif [a] s'applique au PS de type "C" uniquement, tel que défini dans l'EN 50131-6. [b] comme dans l'EN 50131-6, 4.2.5.				

8.1.5 Entrée pour l'utilisateur

Le CIE doit fournir le moyen de recevoir des informations en provenance des dispositifs d'entrée pour l'utilisateur (par exemple: clavier numérique ou commutateur).

8.1.6 Masquage

Le CIE doit fournir le moyen de recevoir des signaux ou des messages de masquage en fonction du grade.

Le CIE doit traiter les signaux ou messages de masquage lorsque le système est hors service et facultativement lorsque celui-ci est mis en service.

8.1.7 Réduction de la plage de détection du détecteur de mouvement

Le CIE doit fournir le moyen utilisé pour recevoir les signaux ou messages de réduction de la plage de détection en fonction du grade.

NOTE Le moyen de transmission des signaux ou messages de réduction de la plage de détection du détecteur de mouvement peut ne pas permettre de différencier les événements de masquage. Voir les normes relatives aux détecteurs.

8.1.8 Entrées non I&HAS

Lorsqu'un CIE reçoit des signaux ou des messages ou d'autres informations qui ne sont pas tenus de satisfaire aux exigences de la présente norme (par exemple: surveillance d'un équipement non I&HAS), cela ne doit avoir aucune incidence sur la capacité du CIE à répondre aux exigences de la présente norme.

8.2 Sorties

Les exigences relatives aux sorties de notification sont détaillées en 8.6.

Le CIE peut avoir besoin de fournir des signaux ou des messages de sortie pour s'interfacer avec d'autres composants de l'I&HAS comme requis par d'autres normes applicables relatives aux composants. La documentation d'installation doit identifier les configurations disponibles.

EXEMPLES:

a) indication activée pour détecteur ou autre composant;

b) information d'état en service/mis hors service pour le détecteur, dispositif de sécurité par brouillard anti-intrusion, etc.;

c) pour déclencher un équipement de confirmation d'alarme sonore ou visuelle;

d) pour déclencher des dispositifs de sécurité par brouillard anti-intrusion, etc.;

e) pour activer le mode essai fonctionnel du détecteur;

f) pour déclencher l'autotest à distance du détecteur ou d'un autre composant;

g) pour restaurer les détecteurs ou d'autres dispositifs.

NOTE Si la restauration implique que les détecteurs ne soient plus alimentés, il convient de laisser s'écouler jusqu'à 180 s pour que le détecteur reprenne son fonctionnement normal (voir la série CEI 62642-2).

Des signaux ou des messages de sortie peuvent également être fournis pour s'interfacer avec les équipements à l'extérieur de l'I&HAS (par exemple: éclairage).

8.3 Fonctionnement

Le CIE doit fournir les moyens nécessaires pour permettre à des utilisateurs autorisés d'accéder aux fonctions du CIE. L'accès à ces fonctions doit être restreint par des niveaux d'accès et des autorisations correspondantes conformément aux 8.3.1 et 8.3.2 (par exemple en utilisant un clavier numérique ou un verrou).

8.3.1 Niveaux d'accès

L'accès aux fonctions d'un CIE doit être restreint conformément aux exigences de la CEI 62642-1, 8.3.1. Si le CIE inclut des fonctions de sécurité complétant celles identifiées dans le Tableau 2 de la CEI 62642-1, les niveaux d'accès nécessaires à l'exploitation de ces fonctions doivent être spécifiés par le fabricant. Les niveaux d'accès pour toutes les fonctions autres que les fonctions de sécurité doivent être spécifiés dans la documentation du fabricant.

L'accès au niveau 3 doit être autorisé par le niveau d'accès 2 tel que:

a) l'accès reste autorisé jusqu'à sa suppression manuelle,

ou

b) l'accès nécessite une autorisation à chaque occasion d'utilisation.

L'accès au niveau 4 doit être autorisé par les niveaux d'accès 2 et 3 à chaque occasion d'utilisation.

Si un accès de niveau 3 est accordé sans une autorisation de niveau 2, comme le permet la CEI 62642-1, 8.3.1, le dispositif d'avertissement interne doit être limité dans le temps, soit à une durée fixe indiquée par le fabricant, soit jusqu'à ce qu'il soit désactivé par l'utilisateur de niveau 3.

8.3.2 Autorisation

L'accès aux fonctions d'un CIE (tel que défini) aux niveaux 2, 3 et 4 doit être restreint comme requis par la CEI 62642-1, 8.3.2. L'autorisation n'est pas requise pour l'accès au niveau 1.

L'autorisation doit être validée par le CIE.

NOTE Si un moyen est prévu pour donner une autorisation temporaire (par exemple code d'identification personnel valable pour une durée limitée ou valable pour une utilisation pendant un nombre spécifié de fois), il convient d'inclure les détails dans la documentation du fabricant.

8.3.2.1 Utilisation de la clé mécanique

Lorsque des clés mécaniques sont utilisées, le fabricant doit fournir des informations suffisantes pour déterminer le nombre de combinaisons disponibles.

8.3.2.2 Utilisation de clés logiques

Lorsque des clés logiques sont utilisées, le fabricant doit fournir des informations suffisantes pour déterminer le nombre de combinaisons disponibles.

De plus, ce qui suit s'applique à des types spécifiques de clés logiques. Cela ne restreint PAS l'utilisation d'autres types.

8.3.2.2.1 Utilisation des codes d'identification personnels

Lorsque des codes d'identification personnels sont utilisés, le nombre de combinaisons non disponibles doit être identifié par le fabricant et ne doit pas être pris en compte dans le calcul des codes disponibles.

Un moyen doit être prévu pour empêcher la lecture des codes d'autorisation.

L'entrée d'un code doit être achevée dans les 60 s. Si l'entrée du code n'est pas terminée dans ce délai, celui-ci doit être traité comme étant invalide dans le contexte du 8.3.2.4.

8.3.2.2.2 Clés numériques

Lorsqu'un utilisateur peut achever la procédure de mise en service et de mise hors service depuis un lieu éloigné de plus de 1 m du CIE ou de l'ACE, des clés numériques utilisées pour l'I&HAS de grades 3 et 4 doivent inclure un moyen permettant d'empêcher l'acceptation de clés copiées à partir de données interceptées (par exemple: codes aléatoires).

Lorsque l'opération peut être réalisée autrement qu'au point de sortie des locaux, un moyen doit être prévu pour rendre les indications “empêchement de mise en service” et “achèvement de mise en service” disponibles à l'utilisateur (par exemple: sur la clé).

Les clés numériques à alimentation propre doivent surveiller la charge du dispositif de stockage comme requis par l'EN 50131-6, 4.2.2 et indiquer la décharge de la batterie au CIE (via l'ACE suivant le cas) chaque fois que le dispositif est utilisé pour la mise en service ou la mise hors service. Ce compte-rendu doit être effectué à chaque événement pour un minimum de 25 événements de cette nature, sur une période n'excédant pas 1 mois et doit entraîner une indication et une entrée dans le journal d'événements (y compris l'identité de l'utilisateur correspondant) chaque fois qu'il est fait état de la condition.

Lorsqu'une condition de décharge de la batterie est identifiée au moment de la mise en service, l'I&HAS ne doit pas se mettre en service jusqu'à ce que l'indication de décharge de la batterie ait fait l'objet d'une validation manuelle au niveau du CIE ou de l'ACE. Cette validation doit être enregistrée au grade 2 et grades supérieurs.

8.3.2.2.3 Clés biométriques

Lorsque des moyens biométriques sont utilisés pour l'autorisation, la structure de codage de reconnaissance doit fournir un nombre minimal de combinaisons comme le montre le Tableau 2. Chaque information de reconnaissance présentée au système doit être comparée à cette structure. Les taux de fausses acceptations et de faux rejets ne doivent pas excéder les valeurs qu'indique le Tableau 2.

Tableau 2 – Reconnaissance des clés biométriques

	Grade 1	Grade 2	Grade 3	Grade 4
Nombre de combinaisons	1 000	10 000	100 000	1 000 000
Taux de fausse acceptation (FAR)	< 0,1 %	< 0,1 %	< 0,01 %	< 0,001 %
Taux de faux rejet (FRR)	< 1 %	< 1 %	< 1 %	< 1 %

Si les FAR et FRR sont ajustables, les moyens de réglage doivent permettre l'identification des paramètres pour garantir une conformité avec les grades ci-dessus. Cette information doit être incluse dans la documentation du fabricant.

NOTE Il convient de prendre en considération les caractéristiques supplémentaires de types spécifiques de dispositifs biométriques en fonction du caractère approprié au risque estimé de l'I&HAS (par exemple: facilité avec laquelle la caractéristique biométrique peut être altérée).

8.3.2.3 Utilisation de méthodes d'autorisation en combinaison

Au moins deux dispositifs ou technologies peuvent être utilisés par une ou plusieurs personnes pour autoriser un accès de niveau 2 ou 3 à un CIE (par exemple: utilisation d'un code d'identification personnel plus clé numérique).

La combinaison des opérations doit être validée par le CIE.

La durée maximale entre l'achèvement d'une opération et le commencement de la suivante doit être restreinte par grade conformément au Tableau 3:

Tableau 3 – Intervalles de temps pour les méthodes d'autorisation utilisées en combinaison

	Grade 1	Grade 2	Grade 3	Grade 4
Durée autorisée	1 min	1 min	30 s	15 s

Le nombre de combinaisons pour chaque dispositif est multiplié pour estimer la conformité de grade qui en découle.

NOTE 1 Deux technologies différentes peuvent être utilisées par la même personne.

NOTE 2 Deux dispositifs de même technologie peuvent être affectés à des personnes différentes.

NOTE 3 Deux technologies peuvent être combinées dans un dispositif unique (par exemple: clé mécanique avec clé numérique intégrée).

8.3.2.4 Détection de tentatives répétées de demandes d'autorisation invalides

En fonction du grade, lorsqu'un CIE utilise des clés logiques pour restreindre l'accès ou lorsque le CIE dispose des moyens lui permettant d'identifier des clés mécaniques individuelles, un moyen doit être prévu pour détecter et enregistrer des tentatives répétées d'accès non reconnues comme étant valides par le CIE, comme spécifié dans le Tableau 4.

Lorsque le Tableau 4 l'exige, le ou les dispositif(s) d'entrée pour l'utilisateur au niveau duquel ou desquels les tentatives invalides sont faites doit ou doivent être mis hors service pendant une durée minimale de 90 s. D'autres dispositifs d'entrée pour l'utilisateur ou l'ensemble d'entre eux peuvent également être mis hors service.

Le dispositif d'auto surveillance ne doit pas être activé lorsque moins de 3 tentatives invalides sont détectées.

Le CIE peut traiter une utilisation répétée de la même clé logique invalide comme une seule tentative.

Tableau 4 – Détection de tentatives répétées de demandes d'autorisation invalides

	Grade 1	Grade 2	Grade 3	Grade 4
Mise hors service du ou des dispositif(s) d'entrée utilisateur	Op	Op [a]	M	M
Nombre maximal de tentatives avant mise hors service initiale du ou des dispositif(s) d'entrée utilisateur	10	10	10	3
Nombre maximal de tentatives supplémentaires avant mise hors service du ou des dispositif(s) d'entrée utilisateur	10	10	1	1
Enregistrement dans le journal d'événements à chaque mise hors service du ou des dispositif(s) d'entrée utilisateur	Op	Op	Op	M
Signal ou message d'auto-surveillance	Op	Op [a]	Op	M
Nombre maximal de tentatives avant activation du dispositif de détection d'auto-surveillance	21	21	21	7
M = Obligatoire Op = Facultatif [a] Pour le grade 2 au moins une de ces exigences doit être prévue.				

8.3.3 Procédures de mise en service

Le CIE doit fournir un moyen permettant à un utilisateur de mettre en service l'I&HAS ou une partie de celui-ci conformément à la CEI 62642-1, 8.3.3 et 8.3.4.

NOTE 1 Il n'est pas obligatoire de fournir un moyen permettant de mettre en service un HAS ou la partie HAS d'un I&HAS.

Le CIE peut fournir un moyen de mise en service automatique à un moment prédéterminé (fonction du temps). Lorsqu'un moyen de mise en service automatique à un moment prédéterminé est fourni, le CIE doit générer au moins une indication avant que la mise en service ne commence. Les détails relatifs à la ou aux indication(s) préliminaire(s) à la mise en service doivent être inclus dans la documentation du fabricant.

NOTE 2 Il convient que cette indication permette à un utilisateur dans les locaux d'être informé de la mise en service imminente de l'I&HAS.

Si une mise en service au grade 1 est mise en œuvre comme le permet la CEI 62642-1, 8.3.4, un moyen doit être fourni pour annuler la procédure de mise en service avant qu'elle ne se termine. Celui-ci ne doit pas permettre l'annulation de la procédure de mise en service si celle-ci est démarrée par d'autres moyens.

8.3.3.1 Interdiction de mise en service et annulation de l'interdiction de mise en service

Le CIE doit fournir un moyen permettant d'interdire la mise en service du système conformément à la CEI 62642-1, 8.3.5 et peut fournir un moyen permettant d'annuler cette interdiction de mise en service conformément à la CEI 62642-1, 8.3.6.

Lorsque la condition d'interdiction de mise en service se produit après que la procédure de sortie a commencé, un moyen doit être fourni afin d'avertir l'utilisateur que la mise en service a été interdite (par exemple: indication par une alarme sonore).

Lorsque la mise en service est fonction du temps, un moyen peut être fourni afin d'annuler les conditions interdisant automatiquement la mise en service.

L'annulation de l'interdiction des conditions de mise en service doit être enregistrée comme le spécifie le 8.10.

8.3.3.2 Fonction de dernière issue

Une fonction de dernière issue est facultative.

Lorsqu'une fonction de dernière issue est prévue, le CIE doit disposer d'un moyen lui permettant de sélectionner le(s) point(s) d'alarme défini(s) à inclure dans la fonction de dernière issue.

Le CIE peut fournir le moyen permettant d'indiquer que la procédure de sortie a commencé conformément à la CEI 62642-1, 8.3.4 et au Tableau 9.

8.3.3.3 Echec de mise en service

Un moyen doit être prévu afin d'indiquer et/ou notifier un échec à la mise en service du CIE à la suite du lancement de la procédure de mise en service.

8.3.3.4 Etat de mise en service

Le CIE doit fournir un moyen limité dans le temps (par exemple, signal ou message de sortie) pour indiquer la mise en service du système (conformément à la CEI 62642-1, 8.3.7).

Un moyen doit être fourni pour la conformité à au moins une des exigences spécifiées dans la CEI 62642-1, 8.3.7 pendant que l'I&HAS (ou une partie de celui-ci) se trouve dans l'état de mise en service.

8.3.4 Procédure de mise hors service

Le CIE doit fournir un moyen permettant à un utilisateur de mettre hors service l'I&HAS ou une partie de celui-ci conformément à la CEI 62642-1, 8.3.3 et 8.3.8.

NOTE Il n'est pas obligatoire de fournir un moyen permettant de mettre hors service un HAS ou la partie HAS d'un I&HAS.

Le CIE peut fournir un moyen permettant la mise hors service à un moment prédéterminé. Lorsque cela est réalisé, la mise hors service automatique ne doit pas annuler une condition d'alarme existante.

Les procédures de mise hors service avec les indications associées, incluant l'utilisation facultative d'une fonction de première issue, doivent être conformes aux exigences de la CEI 62642-1, 8.3.8.

8.3.5 Fonction de restauration

Le CIE doit fournir un moyen permettant de restaurer les conditions comme le définit la CEI 62642-1, 8.3.9.

8.3.6 Fonction d'inhibition

Les fonctions d'inhibition peuvent être appliquées à des alarmes individuelles, de défaut, de fraude ou de hold-up comme défini dans la CEI 62642-1, 8.3.10.

A la prochaine mise en service ou mise hors service du CIE, les conditions d'inhibition doivent être annulées.

Lorsque des fonctions d'inhibition sont prévues, le fabricant doit inclure les détails dans la documentation.

8.3.6.1 Fonction d'inhibition automatique

La fonction d'inhibition peut être réalisée automatiquement, à l'exception des fonctions relatives au système d'alarme contre les hold-up.

Lorsque cette fonction est prévue, la documentation du fabricant doit spécifier le nombre d'occurrences de chaque type d'événement au cours d'une période donnée de mise en service ou de mise hors service avant l'application de l'inhibition.

8.3.7 Opération d'isolation

Les fonctions d'isolation peuvent être appliquées à des alarmes individuelles, de défaut, de fraude ou de hold-up; l'accès à ces moyens doit être restreint conformément à la CEI 62642-1, 8.3.11.

8.3.8 Vérification des fonctions de l'I&HAS

Le CIE doit inclure un moyen permettant à un utilisateur, au niveau d'accès 2, de réaliser un essai fonctionnel sur le ou les dispositif(s) du système d'alarme contre les hold-up et les détecteurs d'intrusion, à condition que ces essais ne rendent pas le dispositif inapte au fonctionnement. De plus, le CIE peut comporter des moyens permettant de réaliser des essais sur le WD ou d'autres composants.

La fonction d'auto surveillance n'est pas l'objet de cet essai: le CIE doit continuer à traiter les signaux ou les messages d'auto surveillance comme le décrit la CEI 62642-1, 8.4.3 durant un tel essai.

Au grade 4, le CIE doit prévoir l'initialisation à distance des autotests réalisés sur les composants du système, tels que requis par les normes applicables relatives aux composants.

NOTE L'affichage d'informations en se trouvant dans des conditions d'essai n'est PAS considéré comme étant une indication dans le cadre de la CEI 62642-1, Tableaux 8 et 9.

8.3.9 Mode d'essai d'immersion du point d'alarme

Afin de fournir un outil pour la maintenance de l'I&HAS, le CIE peut comporter une fonction essai d'immersion. Lorsque celle-ci est prévue, des signaux ou des messages d'alarme en provenance d'un ou plusieurs points d'alarme en essai doivent continuer à être enregistrés dans le journal d'événements.

L'attribut d'immersion peut être manuellement ou automatiquement supprimé. La documentation du fabricant doit spécifier les critères concernant la suppression automatique de l'attribut de l'essai d'immersion et la période de temps au cours de laquelle elle est appliquée (si non programmable). L'accès permettant d'activer et de désactiver manuellement la fonction essai d'immersion doit être restreint au niveau d'accès 3 pour l'ensemble des grades.

L'indication selon laquelle les composants font l'objet d'un essai d'immersion doit être disponible aux utilisateurs aux niveaux d'accès 2 et 3 et la condition doit être indiquée à un utilisateur lors de la mise en service du système.

8.3.10 Autres fonctions

En plus des fonctions normales décrites dans la présente spécification, le CIE peut fournir des fonctions supplémentaires. Une liste doit être fournie dans la documentation du fabricant.

8.4 Traitement

Le CIE doit comporter les moyens nécessaires au traitement des signaux ou des messages d'entrée et générer les signaux ou messages de sortie, les indications ainsi que les notifications comme requis par la CEI 62642-1, 8.4.

NOTE Pour que le CIE traite des conditions de défaut générées en interne, il est supposé que les défauts n'ont pas affecté la capacité du CIE à assurer cette fonction.

8.4.1 Traitement des signaux ou des messages d'entrée

Les signaux ou messages de défaut, d'auto surveillance, des systèmes d'alarme contre les hold-up et d'intrusion doivent être traités pour fournir les notifications requises par la CEI 62642-1, 8.4 et Tableau 7.

En fonction du grade, les événements relatifs au masquage et à la réduction de la plage de détection des détecteurs de mouvement doivent faire l'objet d'un traitement similaire conformément à la CEI 62642-1, 8.4.3 ou 8.4.4 et Tableau 7. Les instructions du fabricant doivent indiquer les modalités de traitement des signaux ou messages relatifs au masquage et à la réduction de la plage de détection.

8.4.1.1 Entrées d'alarme

Les signaux ou messages d'alarme relatifs à une intrusion doivent faire l'objet d'un traitement

a) individuellement pour générer une ou plusieurs conditions d'alarme relative à une intrusion,

ou

b) une condition d'alarme peut être générée par la combinaison logique de signaux ou de messages dans une fenêtre temporelle définie à partir du même point d'alarme ou de points d'alarme groupés logiquement.

8.4.1.2 Priorités

La priorité par défaut du CIE en ce qui concerne le traitement du signal ou du message doit être décrite dans la documentation du fabricant. Dans le cas de la présence simultanée de signaux ou de messages multiples, l'ensemble de ces signaux ou messages doit être traité et au moins un des signaux ou messages de priorité plus élevée doivent faire l'objet d'une notification comme requis par le 8.6.

NOTE Ce détecteur peut donner la priorité à des signaux ou messages multiples en provenance d'un seul détecteur conformément aux recommandations d'une norme relative aux détecteurs.

8.4.2 Traitement des entrées utilisateur

Lorsque des fonctions sont prévues pour permettre à un utilisateur d'entrer des ordres à d'autres dispositifs que le CIE ou de l'ACE, le traitement doit vérifier que les fonctions sélectionnées sont autorisées conformément au 8.3.2.

8.4.3 Surveillance du traitement du CIE

Dans un CIE comportant un traitement des données commandé par un programme, des moyens doivent être prévus pour surveiller la fonction de traitement et fournir un signal approprié conformément au Tableau 5.

Une fonction de surveillance du traitement doit être prévue (par exemple: watchdog), qui doit détecter une défaillance complète de la fonction de traitement dans les 10 s et tenter de relancer le traitement.

En cas de succès, le CIE doit reprendre son fonctionnement dans son mode de fonctionnement antérieur (par exemple: en service ou mis hors service) et cet événement doit être enregistré et indiqué.

Un signal de sortie dédié doit être prévu; celui-ci doit changer d'état dans les 30 s de la détection de la défaillance de traitement, à moins que le CIE n'ait déjà retrouvé son mode de fonctionnement antérieur après relance. Une fois activé, la sortie doit demeurer jusqu'à ce que le CIE ait retrouvé son mode de fonctionnement antérieur.

NOTE S'il ne peut être redémarré, l'I&HAS reste inactif.

Tableau 5 – Surveillance du traitement

	Grade 1	Grade 2	Grade 3	Grade 4
Fonction de surveillance du traitement	Op	Op	M	M
Signal de sortie de défaillance de traitement	Op	Op	Op	M
M = Obligatoire Op = Facultatif				

8.5 Indication

8.5.1 Généralités

Des indications doivent être fournies et affichées conformément aux exigences de la CEI 62642-1, 8.5.1, 8.5.2 et 8.5.3.

Le fabricant doit indiquer comment un utilisateur de niveau 2, 3 ou 4 peut annuler des informations affichées dont l'affichage n'est pas autorisé au niveau d'accès 1.

NOTE 1 Cela peut être réalisé au moyen d'une opération temporisée automatique.

Les indications présentées dans le Tableau 6 complètent celles indiquées dans la CEI 62642-1, Tableau 8.

Tableau 6 – Indications complétant celles de la CEI 62642-1

Indication	Grade 1	Grade 2	Grade 3	Grade 4
Défaillance du traitement du CIE (après relance réussie)	Op	Op	M	M
Défaut de sortie d'alimentation	Op	Op	M	M
Cause de l'interdiction de mise en service	M	M	M	M
M = Obligatoire Op = Facultatif				

Lorsque des voyants partagent des moyens de communication, une indication en attente doit être prévue lorsque d'autres informations sont disponibles pour affichage (par exemple: affichage à cristaux liquides).

Des moyens doivent être fournis pour commander une indication d'alerte destinée aux utilisateurs au niveau d'accès 1 afin d'indiquer que des informations sont disponibles pour les autres niveaux d'accès (par exemple: signal audible ou indicateur visuel clignotant).

Lorsqu'un événement active plus d'une indication, une indication au minimum doit rester jusqu'à ce que la cause soit levée.

NOTE 2 Les indications en attente et d'alerte sont décrites dans la CEI 62642-1.

NOTE 3 Si un tableau synoptique est utilisé, les indications peuvent être disponibles sans restriction afin de fournir un outil de gestion de la sécurité. Dans ce cas, suivant les besoins spécifiques de l'installation, il convient que l'accès général au tableau synoptique soit restreint (par exemple: salle de sécurité intérieure, armoire intérieure fermée à clé).

NOTE 4 L'affichage d'informations dans le mode essai n'est PAS considéré comme étant une indication dans le cadre de la CEI 62642-1, Tableaux 8 et 9.

Le masquage et la réduction de la plage de détection doivent être indiqués de la même manière que les conditions d'intrusion ou de défaut en fonction de leur mode de traitement. En fonction du mode d'indication de ces conditions par le détecteur, il peut ne pas être possible de les différencier au niveau du CIE (voir les normes relatives aux détecteurs).

8.5.1.1 Indications de défaut, de fraude et d'alarme

Les indications de défaut, de fraude et d'alarme doivent nécessiter une annulation (validation) par un utilisateur conformément aux exigences de la CEI 62642-1, 8.5.3.

8.5.1.2 Autres conditions

Les conditions autres que défaut, fraude et alarme doivent être indiquées lors de la mise en service et de la mise hors service et lorsqu'un utilisateur le requiert.

8.5.2 Indicateurs visuels

Lorsque des couleurs sont utilisées pour différencier les alarmes, alors les exigences de la CEI 60073 doivent s'appliquer.

8.5.3 Priorité des indications

Lorsque des voyants partagent des moyens de communication, les indications doivent recevoir un ordre de priorité conformément aux spécifications du fabricant.

8.6 Sorties de notification

Le CIE doit fournir un ou plusieurs signaux ou messages de sortie pour répondre aux exigences décrites dans la CEI 62642-1, 8.6. La documentation du CIE doit indiquer l'option ou les options pouvant être satisfaites.

De plus, si des moyens sont prévus pour avoir un accès de niveau 3 sans une autorisation de niveau 2 (comme le permet la CEI 62642-1, 8.3.1), un moyen doit être fourni pour notifier à distance un "accès de niveau 3" aux grades de sécurité 2 et 3.

Lorsque le CIE fournit des signaux ou des messages de sortie pour SPT et les WD, des moyens peuvent être prévus pour retarder ou supprimer le fonctionnement des WD comme le décrit la CEI 62642-1, 8.6.

Des moyens doivent être prévus pour retarder la notification d'un défaut EPS de 1 h au maximum. Cette notification doit être annulée si le défaut EPS a été corrigé au cours de cette période de retard.

NOTE Il convient que la possibilité d'intégration d'un retard dans le SPT soit prise en compte dans cette fonctionnalité, car certains SPT peuvent inclure un retard; il est donc conseillé de l'introduire dans le paramétrage du retard dans le CIE pour éviter de dépasser la durée maximale permise.

8.6.1 Autre notification

Le CIE peut fournir d'autres signaux ou messages de sortie de notification. Ceux-ci ne doivent pas affecter le respect des exigences de la présente norme.

8.7 Sécurité contre la fraude (détection/protection)

L'ensemble des connexions au CIE doit être contenu dans le ou les boîtier(s) du CIE et l'ensemble des connexions de l'ACE doit être contenu dans le ou les boîtier(s) de l'ACE. Le ou les boîtier(s) du CIE et de l'ACE doivent être dotés d'un moyen permettant d'interdire l'accès aux éléments internes afin de réduire le plus possible les risques de fraude en fonction du grade du CIE.

En ce qui concerne les exigences relatives à la détection et à la protection contre la fraude, les ACE entrent dans les catégories suivantes:

Type A: L'accès aux éléments internes résultant de l'endommagement du boîtier ne pourrait pas permettre de modifier l'état d'une partie quelconque de l'I&HAS ou interdire le déclenchement d'une notification obligatoire (par exemple: dispositif en résine coulée);

Type B: L'accès aux éléments internes résultant de l'endommagement du boîtier pourrait permettre de modifier l'état d'une partie quelconque de l'I&HAS ou interdire le déclenchement d'une notification obligatoire (par exemple: ACE comportant des connexions pour les détecteurs).

8.7.1 Protection contre la fraude

La construction du ou des boîtier(s) du CIE et de l'ACE doit satisfaire aux exigences en matière de protection contre la fraude de la CEI 62642-1 ainsi qu'aux exigences relatives aux impacts pour le grade correspondant conformément au Tableau 7. Les degrés de protection contre les impacts IK sont détaillés dans la CEI 62262.

Cette exigence autorise l'endommagement du boîtier mais un signal d'auto surveillance doit être généré avant qu'un accès non autorisé aux éléments internes ne soit possible (sauf pour les dispositifs de type A).

Lorsque le CIE est réparti dans le boîtier d'autres composants de l'I&HAS, alors la protection contre la fraude de ces boîtiers doit être conforme à la présente norme.

Les moyens d'accès aux éléments internes d'un CIE ou d'un ACE doivent être robustes et sécurisés mécaniquement.

Tableau 7 – Protection contre la fraude

		Grade 1		Grade 2		Grade 3		Grade 4	
		Int	Ext	Int	Ext	Int	Ext	Int	Ext
CIE	Niveau de sévérité (code IK) (spécification de conception)	04	NA	06	NA	06	NA	06	NA
	Energie d'impact (Joule) (condition d'essai)	0,5	NA	1	NA	1	NA	1	NA
ACE Type A	Niveau de sévérité (code IK) (spécification de conception)	04	07	04	07	04	07	04	07
	Energie d'impact (Joule) (condition d'essai)	0,5	2	0,5	2	0,5	2	0,5	2
ACE Type B	Niveau de sévérité (code IK) (spécification de conception)	04	07	06	08	06	08	06	08
	Energie d'impact (Joule) (condition d'essai)	0,5	2	1	5	1	5	1	5

NA = non applicable.
Int = à l'intérieur des locaux surveillés.
Ext = à l'extérieur des locaux surveillés (intérieur ou extérieur).

Ces exigences ne sont pas applicables aux ACE portables.

Pour les grades 1 et 2, cette exigence n'inclut pas les voyants ou les organes de commande (par exemple: boutons-poussoirs, claviers numériques, écrans à cristaux liquides ou écrans graphiques); pour les grades 3 et 4, de tels voyants et organes de commande sont inclus, lorsqu'un utilisateur de niveau 1 peut y avoir accès.

8.7.2 Détection de la fraude

Que le CIE/l'ACE soit autonome dans son propre boîtier ou soit réparti dans le ou les boîtier(s) d'autres composants de l'I&HAS, un signal ou un message d'auto surveillance doit être généré conformément aux exigences spécifiées dans le Tableau 8 avant qu'un accès ne soit possible pour annuler la détection.

Tableau 8 – Détection de la fraude

Evénement à détecter	Grade 1	Grade 2	Grade 3	Grade 4
Accès à l'intérieur du boîtier [a]	M	M	M	M
Enlèvement du support	Op	Op	M	M
Enlèvement du support (composants du système sans fil)	Op	M	M	M
Pénétration dans le boîtier [b]	Op	Op	Op	M

M = Obligatoire Op = Facultatif NA = Non applicable.

[a] Non applicable au dispositif de type A.

[b] Lorsqu'il se trouve à l'extérieur des locaux surveillés.

Ces exigences ne sont pas applicables aux ACE portables.

8.7.2.1 Accès à l'intérieur du boîtier

L'ouverture du boîtier du CIE/de l'ACE de type B en utilisant des moyens usuels doit générer un signal ou un message d'auto surveillance.

Le boîtier ne doit pas autoriser l'introduction d'outils de dimensions spécifiées dans le Tableau 9 pour faire échec à la détection de la fraude avant que celle-ci ait été activée.

Tableau 9 – Dimension des outils pour la détection de la fraude

Outil	Grade 1	Grade 2	Grade 3	Grade 4
Tige d'acier comme spécifié dans la CEI 60529, avec diamètre	2,5 mm	2,5 mm	1 mm	1 mm
Barre plate de dimensions	10 × 1 × > 300 mm	10 × 1 × > 300 mm	5 × 0,5 × > 300 mm	5 × 0,5 × > 300 mm
Fil d'acier, résistance à la traction 650 - 825 MPa et dimensions	NA	NA	1 mm dia × 300 mm	1 mm dia × 300 mm
NA = Non applicable				

Cette exigence n'est pas applicable aux dispositifs de type A.

Pour les grades 1 et 2, cette exigence n'inclut pas l'introduction d'un outil via les voyants ou les organes de commande (par exemple: boutons-poussoirs, claviers numériques, écrans à cristaux liquides ou écrans graphiques) ou autres ouvertures; pour les grades 3 et 4, de tels voyants, organes de commande et toute autre ouverture accessibles à un utilisateur de niveau 1 sont inclus.

8.7.2.2 Enlèvement du support

Des tentatives d'enlèvement du CIE/de l'ACE de type B de sa surface de montage pour une distance supérieure à celle définie dans le Tableau 10 doit générer un signal ou un message d'auto surveillance conformément au Tableau 8.

Il convient qu'il soit impossible de faire échec à la détection d'un enlèvement du système de son support en glissant une lame de 25 × 1 × > 300 mm ou en utilisant des pinces (d'épaisseur 5 mm et de portée 150 mm) entre la surface de montage et le CIE/l'ACE.

Tableau 10 – Enlèvement du support

	Grade 1	Grade 2	Grade 3	Grade 4
Distance maximale avant détection de la fraude	10 mm	10 mm	5 mm	5 mm

8.7.2.3 Pénétration dans le boîtier

Lorsque celui-ci est monté conformément aux instructions du fabricant, il doit être impossible de pénétrer dans le boîtier du CIE/de l'ACE de type B par n'importe laquelle de ses faces accessibles avec un outil métallique créant un trou de 4 mm ou de diamètre supérieur sans générer un signal ou un message d'auto surveillance.

NOTE Le but est de détecter une diminution de l'intégrité originelle du boîtier. La définition du diamètre du trou a pour but de fixer un seuil objectif pour la vérification des performances et de la conception du produit.

8.7.3 Surveillance de la substitution

Le CIE de grade 4 doit fournir les moyens de surveiller la substitution des composants de l'I&HAS comme requis par la CEI 62642-1, 8.7.3 et 8.7.4.

8.8 Interconnexions

Le CIE doit comporter des moyens permettant de vérifier que la fonction d'interconnexion est exécutée normalement comme le décrit la CEI 62642-1, 8.8 (y compris les paragraphes).

Le CIE doit comporter une interface physique et logique pour les interconnexions. La documentation du fabricant doit spécifier le type d'interconnexion supporté comme l'indique l'Annexe A.

NOTE 1 Les normes relatives aux composants de l'I&HAS spécifient les exigences de certaines interconnexions.

NOTE 2 La CEI 62642-5-3 spécifie les exigences pour les interconnexions sans fil.

8.9 Caractéristiques temporelles

Les signaux et les messages doivent être traités comme le spécifie la CEI 62642-1, 8.9 (paragraphes compris).

Des caractéristiques temporelles doivent être appliquées aux conditions de masquage et de réduction de la plage de détection selon qu'elles sont traitées comme des événements d'intrusion ou de défaut.

NOTE 1 L'immunité à la reconnaissance accidentelle d'un signal ou d'un message d'alarme due à une interférence électrique (par exemple, interférence électromagnétique) est abordée par la directive régionale relative à la compatibilité électromagnétique.

NOTE 2 L'Annexe B inclut un résumé des exigences temporelles.

8.10 Enregistrement d'événements

Les événements doivent être enregistrés conformément à la CEI 62642-1, 8.10.

NOTE Le décompte du nombre d'événements enregistrés à partir d'une seule source lors d'une période de mise hors service peut être réinitialisé à zéro dans le cas d'une opération de restauration de niveau d'accès 3.

Le CIE doit comporter des moyens permettant d'enregistrer les événements comme le spécifie le Tableau 22 de la CEI 62642-1 ainsi que les conditions indiquées dans le Tableau 11.

Tableau 11 – Evénements supplémentaires à inclure dans le journal d'événements

Evènements	Grade 1	Grade 2	Grade 3	Grade 4
Dispositif d'entrée désactivé pour la détection de codes répétés d'autorisation invalides	Op	M [a]	M	M
Défaillance du traitement du CIE (après relance réussie)	Op	Op	M	M
Batterie faible, clé logique auto-alimentée	Op	M	M	M
Validation de batterie faible, clé logique auto-alimentée à la mise en service	Op	M	M	M
Masquage [b]	Op	Op	M	M
Réduction de la plage de détection [b]	Op	Op	Op	M
Identification d'interface non I&HAS utilisée (voir Annexe C)	Op	M	M	M

M = Obligatoire Op = Facultatif

[a] Si option sélectionnée - voir Tableau 4.

[b] “Réduction de la plage de détection” peut être impossible à distinguer du “Masquage” (voir la série CEI 62642-2).

8.10.1 Enregistrement d'événements au niveau du CIE

Lorsque des événements sont enregistrés au niveau du CIE, chaque nouvel événement doit être enregistré au cours du temps de traitement autorisé par la CEI 62642-1, 8.9.2

L'enregistrement des événements répertoriés comme étant obligatoire dans le Tableau 11 et dans la CEI 62642-1, Tableau 22, ne doit pas être affecté ou écrasé par l'enregistrement des événements répertoriés comme étant “facultatif” (par exemple: journaux d'événements distincts) si cette opération ramenait le nombre d'événements enregistrés au-dessous du minimum requis par la CEI 62642-1, Tableau 21.

L’enregistrement d'événements supplémentaires, en dehors du domaine d'application de la CEI 62642-1 est autorisé si cette opération ramène le nombre d'événements enregistrés au-dessous du minimum requis par la CEI 62642-1, Tableau 21 et ne doit pas écraser les événements spécifiés par la CEI 62642-1, Tableau 22.

Le temps enregistré avec un événement enregistré doit comporter au minimum les heures et les minutes; la date doit comporter au minimum le jour et le mois.

Lorsque l'exigence relative au temps de stockage de la CEI 62642-1, Tableau 21 est satisfaite par la fourniture d'une batterie de secours de la mémoire, le fabricant du CIE doit spécifier l'intervalle entre les changements de batterie.

Dans le CIE et pour les grades 3 et 4, un dispositif doit être prévu pour enregistrer en permanence le journal d'événements.

NOTE Il n'est pas indispensable que le CIE fournisse un moyen d'enregistrement en permanence du journal d'événements, à condition qu'il soit doté d'un moyen permettant de transférer le journal d'événements à un dispositif externe adéquat (par exemple: une imprimante).

8.10.2 Enregistrement des événements au niveau de l'ARC ou d'un autre lieu déporté

Lorsque l'enregistrement d'événements est assuré au niveau de l'ARC ou d'un autre lieu déporté, le CIE doit fournir un moyen permettant d'indiquer que la transmission des événements au lieu déporté a échoué.

Lorsque le transfert des événements est impossible, pour le grade de sécurité 1, une condition de défaut doit être générée. Pour les grades de sécurité 2, 3 et 4, les événements dont la transmission a échoué doivent être transférés à un composant adapté de l'I&HAS aux fins de stockage jusqu'à ce que le transfert soit possible. Les exigences relatives à cette mémoire temporaire doivent satisfaire aux exigences de la CEI 62642-1, Tableau 21.

8.11 Alimentation

Le CIE peut être alimenté par une PS intégrée ou une PS distincte. Dans l'un ou l'autre cas, les exigences de la CEI 62642-1, 9.2, de l'EN 50131-6 et de la présente norme doivent être satisfaites.

La PS doit être capable d'alimenter le CIE dans toutes les conditions, y compris lors de la recharge des dispositifs de stockage dans les périodes requises.

La documentation du fabricant doit définir la consommation de courant du CIE et de l'ACE.

NOTE Le concepteur du système (installateur) aura besoin de calculer la période totale d'autonomie requise pour l'I&HAS, conformément au grade de l'I&HAS, comme l'indique la CEI 62642-1.

9 Documentation relative au produit

9.1 Installation et maintenance

Les informations spécifiées par la CEI 62642-1, 14.2 doivent être fournies, ainsi que les informations suivantes:

a) température de fonctionnement et plage d'humidité;

b) poids et dimensions;

c) détails relatifs à la fixation;

d) instructions relatives à l'installation, à la mise en service et à la maintenance, y compris l'identification des terminaux;

e) type d'interconnexions (se reporter au 8.8);

f) détails relatifs aux méthodes de mise en service et de mise hors service (se reporter aux 11.7.1 à 11.7.3 et aux Tableaux 23 à 26);

g) lorsqu'il existe des pièces à entretenir (exemple: fusibles) leur type et valeur;

h) exigences en matière d'alimentation en l'absence de PS intégrée;

i) lorsque la PS est intégrée, informations requises par l'EN 50131-6, Article 6;

j) nombre maximal de chaque type d'ACE et dispositif d'extension;

k) consommation de courant du CIE et de chaque type d'ACE et de dispositif d'extension, avec et sans condition d'alarme;

l) courant nominal maximal de chaque sortie électrique;

m) fonctions programmables fournies;

n) moyen par lequel les indications sont rendues inaccessibles aux utilisateurs de niveau 1 lorsque l'utilisateur de niveau 2, 3 ou 4 n'a plus accès aux informations (se reporter au 8.5.1);

o) les signaux/messages de masquage/de réduction de la plage de détection sont-ils traités comme étant des événements de “défaut” ou de “masquage” (se reporter aux 8.4.1, 8.5.1 et au Tableau 11);

p) affectation d'une priorité au traitement des signaux et des messages et indications (se reporter aux 8.4.1.2, 8.5.3);

q) nombre minimal de variations de codes d'identification personnels, de clés logiques, de clés biométriques et/ou de clés mécaniques pour chaque utilisateur (se reporter au 8.3);

r) méthode de programmation temporelle des WD internes pour un accès de niveau 3 sans autorisation de niveau 2 (se reporter au 8.3.1);

s) nombre et détails relatifs aux codes PIN rejetés (se reporter au 8.3.2.2.1);

t) détails relatifs aux méthodes d'autorisation biométrique utilisées (se reporter au 8.3.2.2.3);

u) méthode utilisée afin de déterminer le nombre de combinaisons de codes PIN, de clés logiques, de clés biométriques et/ou de clés mécaniques (se reporter au 11.6);

v) nombre de saisies de code invalide avant que l'interface utilisateur ne soit désactivée (se reporter au 8.3.2.4);

w) détails relatifs aux moyens d'autorisation temporaire pour un accès utilisateur (se reporter au 8.3.2);

x) si une mise en service automatique à des moments prédéterminés est prévue, détails relatifs aux indications de mise en service préliminaire ainsi que toute annulation automatique de l'interdiction de mise en service (se reporter aux 8.3.3, 8.3.3.1);

y) détails relatifs aux conditions prévues pour l'état de mise en service (se reporter au 8.3.3.4);

z) signaux ou messages de sortie de notification fournis (se reporter au 8.6);

aa) autres configurations de sortie pour l'interfaçage avec les composants de l'I&HAS (se reporter au 8.2);

bb) critères pour la suppression automatique de l'attribut de “l'essai d'immersion” (se reporter au 8.3.9);

cc) nombre d'événements entraînant une inhibition automatique (se reporter au 8.3.6.1);

dd) si l’ACE est de type A ou de type B (se reporter au 8.7) et s'il est portable ou déplaçable (se reporter au 11.14);

ee) données relatives aux composants pour les composants de mémoire non volatiles (se reporter au Tableau 30, étape 6);

ff) durée de vie de la batterie de secours pour mémoire (se reporter au 8.10.1);

gg) fonctions facultatives fournies (se reporter au 4.1);

hh) fonctions supplémentaires fournies (se reporter aux 4.2, 8.1.8);

ii) niveaux d'accès requis pour accéder aux fonctions supplémentaires fournies;

jj) détails relatifs à toute fonction programmable qui rendrait un I&HAS non conforme à la CEI 62642-1, 8.3.13 ou conforme à un grade de sécurité moins élevé, accompagnés d'une instruction relative à un retrait de l'étiquetage de conformité qui en résulte (se reporter aux 4.2 et 8.3.10).

9.2 Instructions de fonctionnement

Les informations suivantes doivent être fournies:

a) instructions de fonctionnement pour toutes les fonctions de sécurité et autres fonctions disponibles à l'utilisateur;

b) norme(s) pour laquelle la conformité est demandée pour le produit;

c) grade de sécurité auquel le CIE et l'ACE sont conformes;

d) classe d’environnement;

e) nombre minimal de variations de clés logiques et/ou mécaniques pour chaque utilisateur;

f) nombre de codes rejetés et détails relatifs à ceux-ci;

g) fonctions programmables par l'utilisateur fournies;

h) lorsqu'il existe des pièces à entretenir par l'utilisateur (exemple: fusibles) leur type et leur valeur.

10 Marquage et étiquetage

Le CIE et l'ACE doivent faire l'objet d'un marquage comme requis par la CEI 62642-1,ainsi que d'autres informations requises par des directives réglementaires régionales.

11 Essais

Lorsque les produits doivent être soumis à des essais de conformité à la présente norme, les exigences de l'Article 11 doivent s'appliquer.

Les grades de sécurité 1 à 4 doivent être conformes aux descriptions dans la CEI 62642-1.

Dans le cas du développement d'un composant supplémentaire destiné à être utilisé avec l'équipement déjà soumis à essai ou de la révision de cet équipement, il convient qu'un plan d'essai de révision fasse l'objet d'un accord avec le laboratoire d'essai.

11.1 Conditions d'essai

11.1.1 Conditions en laboratoire et tolérance

Les conditions d'essai doivent être conformes à la CEI 60068-1:1988, 5.3.1, comme suit:

– température: 15 °C à 35 °C
– humidité relative: 25 % à 75 %
– pression d'air: 86 kPa à 106 kPa

11.1.2 Montage

Sauf indication contraire, le CIE/l'ACE doit être monté conformément aux instructions d'installation du fabricant. Pour les essais d'environnement, l'EUT doit être monté dans son orientation opérationnelle correcte. Le matériau utilisé pour la surface de montage ne doit pas influencer les résultats d'essai.

Tout équipement supplémentaire nécessaire à la réalisation des essais (par exemple: simulation des détecteurs ou des dispositifs d'avertissement) doit être fourni par le fabricant en accord avec le laboratoire d'essai.

Tous les signaux/messages d'entrée (par exemple: ligne de BUS ou entrées de détecteurs câblées directement) doivent se terminer correctement conformément aux instructions du fabricant.

11.1.3 Configuration d'essai du CIE

Pour les essais fonctionnels, un CIE dans une configuration représentative doit être fourni comme suit:

a) le CIE doit comporter au moins un ACE de chaque type et 10 % (mais au moins un) de chaque type de dispositif d'extension ou de composant de CIE en réseau pour lequel le fabricant demande les essais;

b) le fabricant doit fournir un équipement au laboratoire d'essai avec des points d'entrées d'alarme connectées comme défini ci-dessous et programmées afin de répondre aux exigences de la présente norme:

- chaque composant périphérique capable d'accepter des entrées de points d'alarme doit avoir 10 % (mais au moins 2) de points d'alarme connectés de chaque type;
- pour les équipements sans fil, au moins 8 points d'alarme sans fil doivent faire l'objet d'un essai;
- si l'une des deux configurations ci-dessus entraîne un nombre supérieur à la capacité du dispositif, toutes les entrées doivent être connectées;
- lorsque plusieurs entrées de type “bus” sont fournies ou qu'un mélange d'entrées filaires et non filaires peut être connecté, les points d'alarme doivent être répartis pour vérifier l'ensemble des bus et des types d'interconnexion;
- il peut exister plusieurs types de composants système périphériques capables d'accepter les connexions d'entrée. Dans ce cas, tous ces types de périphériques doivent être vérifiés;

c) le reste de la configuration de l'I&HAS peut être simulé (par exemple: commutateurs pour simuler les détecteurs, DEL pour simuler les WD);

d) le journal d'événements peut être pré-rempli par le fabricant avant l'essai.

L'EPS et tout APS doivent être connectés conformément aux instructions du fabricant.

Lorsqu'une horloge en temps réel est utilisée conjointement avec un journal d'événements, l'horloge doit être réglée sur l'heure locale.

Le fabricant doit fournir une déclaration selon laquelle la configuration système maximale pour le CIE a été intégralement soumise à un essai en interne.

Une configuration système réduite peut être fournie pour les essais d'environnement et de compatibilité électromagnétique.

11.1.4 Alimentation

Lorsque l'alimentation du CIE est fournie par une PS de type A ou B, l'essai fonctionnel réduit doit être réalisé avec l'EPS à la valeur nominale et avec l'APS à un niveau d'au moins 80 % de la pleine capacité et la connexion doit être effectuée conformément aux instructions du fabricant. Pour un CIE nécessitant un PS de type C, le SD doit se trouver à un niveau d'au moins 80 % de la pleine capacité.

11.1.5 Contrôles du journal d'événements

Des procédures d'essai spécifient le contrôle de journaux d'événements au stade auquel le contrôle est pertinent. Il peut ne pas être pratique d'effectuer le contrôle à ce stade (par exemple: si le CIE doit se trouver dans l'état hors service pour visualiser les événements du journal). Ainsi tous les contrôles de journaux d'événements pour un essai peuvent être réalisés ensemble comme étape finale.

Il convient qu'au moins un contrôle vérifie que le temps spécifié au 8.10.1 soit satisfait.

11.1.6 Documentation

11.1.6.1 Produit

La documentation relative au produit (comme requise à l'Article 9) doit être fournie avec le CIE.

11.1.6.2 Dispositif d'essai du simulateur

Si un équipement supplémentaire (par exemple: un simulateur ou un dispositif programmable) est fourni par le fabricant, les plans de connexion, une description opérationnelle et le mode d'emploi doivent être fournis.

11.2 Procédures d'essai

Tous les essais décrits dans l'Article 11 doivent être réalisés.

NOTE Lorsque des fonctionnalités définies comme étant facultatives dans la présente norme ne sont pas assurées, alors les essais ne sont pas requis.

11.2.1 Tolérances

Lorsque des signaux/messages sont appliqués pendant une durée définie, ceux-ci doivent faire l'objet d'une tolérance de –0 %, +5 %.

Les critères de réussite/d'échec sont donnés dans chaque essai.

11.2.2 Dispositifs sans fil

Les dispositifs sans fil doivent faire l'objet des essais supplémentaires requis par la CEI 62642-5-3.

11.3 Essai fonctionnel réduit

Pour des essais spécifiés (par exemple: essais d'environnement), il peut ne pas être possible ou souhaitable de réaliser un essai fonctionnel complet; dans ce cas, un essai fonctionnel réduit doit être réalisé conformément au Tableau 12.

Tableau 12 – Essai fonctionnel réduit

Etape	Condition d'essai (c)	Action (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	CIE hors service Absence de "signaux et messages de défaut, d'auto surveillance, d'intrusion" Aucune indication active	Appliquer un signal ou un message d'alarme intrusion pendant 401 ms.	Vérifier les indications.	Les indications doivent être conformes au grade (comme l'indique la CEI 62642-1, Tableaux 8 et 9).
2	Comme ci-dessus +: une entrée d'alarme contre l'intrusion, non allouée comme une"fonction de première entrée"	Tenter de mettre en service le système.	Enregistrer si le système se met en service.	Il convient que la mise en service du système soit interdite.
3	Comme dans 1 ci-dessus	Mettre en service le système.	Enregistrer les indications.	Les indications doivent être conformes au grade (comme l'indique la CEI 62642-1, Tableaux 8 et 9).
4	CIE en service	Appliquer un signal ou un message d'alarme comme spécifié au 8.9.	Surveiller les signaux ou les messages de sortie de notification et enregistrer les résultats.	Au moins une configuration de notification requise par la CEI 62642-1, Tableau 10, selon le grade, doit être activée conformément à la CEI 62642-1, Tableau 7.

Etape	Condition d'essai (c)	Action (d)	Mesure (e)	Critères de réussite/d'échec (f)
5	CIE dans “l'état en service” et dans l'état “alarme”	Mettre manuellement hors service le CIE.	Enregistrer si le système a modifié son état en “hors service” et si les messages ou signaux de sortie de notification sont corrects et vérifier le journal d'événements (grades 2, 3 et 4).	CIE hors service Les indications doivent être conformes au grade (comme l'indique la CEI 62642-1, Tableaux 8 et 9). Les sorties WD ne doivent émettre aucun signal, d'autres signaux ou messages de sortie de notification peuvent rester actifs jusqu'à la restauration. Temps correct et séquences d'événement enregistrées
6	CIE dans “l'état hors service”	Restaurer le CIE.	Enregistrer si le système revient à l'état normal.	Conformément au 8.3.5

11.4 Essais fonctionnels

11.4.1 Traitement des signaux ou des messages d'alarme contre l'intrusion

a) Objet de l'essai

L'objet de l'essai est de démontrer la capacité du CIE à être conforme aux 8.1.1, 8.3.5, 8.4.1, 8.4.1.2, 8.5, 8.6, 8.9 et 8.10:

1) recevoir et traiter un signal ou un message d'intrusion conformément aux exigences relatives aux caractéristiques temporelles du traitement de la présente spécification, lorsque le CIE se trouve dans l'état en service et hors service;
2) fournir une ou des indications et une ou des notifications;
3) enregistrer correctement le ou les événements dans le journal d'événements;
4) restaurer conformément au 8.3.5.

b) Principe

L'essai consiste à appliquer un signal/message d'intrusion comme spécifié au 8.9 à une entrée d'intrusion, ainsi qu'à contrôler que l'entrée a été traitée dans la période de temps requise et que l'indication et la ou les notifications correctes se produisent, voir Tableau 13.

Tableau 13 – Essais réalisés sur le traitement des signaux ou des messages d'intrusion

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous avec toutes les entrées et sorties dans l'état normal.		MESURE GENERALE Enregistrer l'état des indications et des notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué Moment où la notification se produit Enregistrer le journal d'événements	CRITERES GENERAUX Le traitement doit être effectué conformément à la CEI 62642-1, Tableau 7 et 8.4.1. Les indications et les notifications doivent être conformes à la CEI 62642-1, Tableaux 8, 9 et 10.
1	CIE en “mode en service”	Appliquer un signal/message d'intrusion pendant 401 ms	Mesure générale + Enregistrer l'identité du point d'alarme activé.	Critères généraux + la notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9. L’enregistrement doit être conforme au 8.10.
2	CIE en “mode en service” (avec condition d'alarme)	Mettre hors service le CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
3	CIE en “mode mise hors service”	Restaurer (exemple: en saisissant un numéro de code PIN correct au clavier numérique)	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou messages multiples appliqués au même point d'alarme sont enregistrés dans le journal d'événements le nombre de fois spécifié dans la CEI 62642-1, 8.10.	Appliquer le même signal/message d'intrusion pendant 401 ms une fois de plus que le nombre maximal de fois spécifié dans la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes contre l'intrusion en provenance de la même source doit être conforme à la CEI 62642-1, 8.10.
5	CIE en “mode hors service” NOTE Pour vérifier que les signaux ou messages d'intrusion ne sont pas enregistrés dans le journal d'événements.	Appliquer le même signal/message d'intrusion pendant 401 ms quatre fois Ensuite, répéter l'étape 3.	Mesure générale	Critères généraux

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en “mode en service”. NOTE Pour vérifier que si des signaux ou des messages multiples sont appliqués, au moins un est traité correctement	Appliquer des signaux ou des messages d'intrusion équivalant à 5 % de la capacité maximale des points d'alarme du CIE ou 5 (selon la valeur la plus importante) en 1 s.	Mesure générale	Au moins un signal ou message d'intrusion doit être traité conformément à 8.4.1.2 et 8.9.
7	CIE en “mode en service” (avec plus d'une condition d'alarme)	Mettre hors service le CIE.	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.1.1.
8	CIE en “mode hors service”	Restaurer toutes les conditions.	Mesure générale	Conformément au 8.3.5

11.4.2 Traitement des signaux ou des messages d'alarme contre les hold-up

a) Objet de l'essai

L'objet de l'essai est de démontrer la capacité du CIE y compris de la fonction d'alarme contre les hold-up à satisfaire des 8.1.2, 8.3.5, 8.4.1, 8.5, 8.6, 8.9, 8.10 et à:

1) recevoir et de traiter un signal ou un message d'alarme contre les hold-up conformément aux exigences relatives aux caractéristiques temporelles du traitement de la présente spécification, lorsque le CIE se trouve dans l'état en service et hors service;

   NOTE Cet essai se réfère à la partie HAS du CIE en service ou hors service. Lorsqu'un mode hors service n'est pas prévu pour HAS, cette partie d'essai n'est pas nécessaire.

2) fournir une ou des indications et une ou des notifications;

3) enregistrer correctement le ou les événement(s) dans le journal d'événements;

4) restaurer conformément au 8.3.5.

b) Principe

L'essai consiste à appliquer un signal d'alarme contre les hold-up comme le spécifie le 8.9 ou un message d'alarme contre les hold-up compatible avec le CIE à une entrée d'alarme contre les hold-up lorsque le système se trouve dans diverses conditions indiquées dans le Tableau 14 ci-dessous. Le système doit faire l'objet d'une surveillance afin de s'assurer que l'entrée a été traitée dans le délai requis et que la ou les indication(s), la ou les notification(s) et enregistrement des événements correct(s) sont intervenus.

Tableau 14 – Essais réalisés sur le traitement des signaux ou des messages d'alarme contre les hold-up

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous, avec toutes les entrées et sorties dans l'état normal.		MESURE GENERALE Enregistrer l'état des indications et notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué Moment où la notification intervient Enregistrer le journal d'événements	CRITERES GENERAUX Le traitement doit être réalisé conformément à la CEI 62642-1, Tableau 7 et 8.4.1. Les indications et notifications doivent être conformes à la CEI 62642-1, Tableaux 8, 9 et 10.
1	CIE en “mode en service”	Appliquer le signal/message d'alarme contre les hold-up pendant 401 ms.	Mesure générale + Enregistrer l'identité du point d'alarme activé.	Critères généraux + Comme défini au 8.9, la notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9 L’enregistrement doit être effectué conformément au 8.10.
2	CIE “en mode en service” (avec condition d'alarme)	Mettre hors service le CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5
3	CIE “en mode hors service”	Restaurer	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou des messages multiples appliqués au même point d'alarme contre les hold-up sont enregistrés dans le journal d'événements le nombre de fois spécifié dans la CEI 62642-1, 8.10.	Appliquer le même signal/message d'alarme contre les hold-up pendant 401 ms une fois de plus que le nombre maximal de fois spécifié dans la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes contre les hold-up en provenance de la même source doit être conforme à la CEI 62642-1, 8.10.
5	CIE en “mode hors service” NOTE Pour vérifier que les signaux ou messages d'alarme contre les hold-up ne sont pas enregistrés dans le journal d'événements.	Appliquer le même signal/message d'alarme contre les hold-up pendant 401 ms quatre fois Ensuite, répéter l'étape 3.	Mesure générale	Critères généraux

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en “mode en service” NOTE Pour vérifier que si des signaux ou messages multiples sont appliqués, au moins un est traité correctement.	Appliquer des signaux ou des messages d'alarme contre les hold-up équivalant à 5 % de la capacité maximale des points d'alarme du CIE ou 5 (selon la valeur la plus importante) en 1 s	Mesure générale	Au moins un signal ou message d'alarme contre les hold-up doit être traité conformément aux 8.4.1.2 et 8.9
7	CIE en “mode en service” (avec plus d'une condition d'alarme)	Mettre hors service le CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.1.1.
8	CIE en “mode hors service”	Restaurer l'ensemble des conditions.	Mesure générale	Conformément au 8.3.5

11.4.3 Traitement des signaux ou messages d'auto surveillance

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme aux 8.1.3, 8.3.5, 8.4.1, 8.5, 8.6, 8.9, 8.10 et à:

1) recevoir et traiter un signal ou un message d'auto surveillance conformément aux exigences relatives aux caractéristiques temporelles du traitement de la présente spécification, lorsque le CIE se trouve dans l'état en service et hors service;
2) fournir une ou des indication(s) et une ou des notification(s);
3) enregistrer correctement le ou les événement(s) dans le journal d'événements;
4) restaurer conformément au 8.3.5.

b) Principe

L'essai consiste à appliquer un signal d'auto surveillance comme le spécifie le 8.9 ou un message d'auto surveillance compatible avec le CIE, à une entrée d’auto surveillance lorsque le système se trouve dans diverses conditions indiquées dans le Tableau 15 ci-dessous. Le système doit faire l'objet d'une surveillance afin de s'assurer que l'entrée a été traitée dans le délai requis et que l'enregistrement correct des événements, de la ou des notifications et des indications a été effectué.

Tableau 15 – Essais réalisés sur le traitement de signaux ou de messages d'auto surveillance

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous, avec toutes les entrées et sorties dans l'état normal. Lorsque des méthodes multiples de mise en service et de mise hors service du CIE sont prévues, alors l'essai doit être réalisé pour chacune des méthodes.		MESURE GENERALE Enregistrer l'état des indications et notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué Moment où la notification intervient Enregistrer le journal d'événements	CRITERES GENERAUX Le traitement doit être réalisé conformément à la CEI 62642-1, Tableau 7 et 8.4.1. Les indications et notifications doivent être conformes à la CEI 62642-1, Tableaux 8, 9 et 10.
1	CIE en “mode en service”	Appliquer le signal/message d'auto surveillance pendant 401 ms	Mesure générale + Enregistrer l'identité du point d'alarme activé.	Critères généraux + Comme défini au 8.9, la notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9 L’enregistrement doit être effectué conformément au 8.10.
2	CIE en “mode en service” (avec condition d'alarme contre la fraude)	Mettre hors service le CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
3	CIE en “mode en service”	Restaurer	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou des messages multiples d'auto surveillance en provenance de la même source sont enregistrés dans le journal d'événements le nombre de fois spécifié dans la CEI 62642-1, 8.10.	Appliquer le même signal/message d'auto surveillance pendant 401 ms une fois de plus que le nombre maximal de fois spécifié dans la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes contre la fraude en provenance de la même source doit être conforme à la CEI 62642-1, 8.10.
5	CIE “en mode hors service”	Appliquer le signal/message d'auto surveillance pendant 401 ms.	Mesure générale + Enregistrer l'identité du point d'alarme activé	Critères généraux + Comme défini au 8.9, la notification (en fonction du grade, se reporter à la CEI 62642-1, Tableau 7) doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9. L’enregistrement doit être effectué conformément au 8.10.

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en “mode hors service” NOTE Pour vérifier que des signaux ou des messages multiples d'auto surveillance en provenance de la même source sont enregistrés dans le journal d'événements le nombre de fois spécifié dans la CEI 62642-1, 8.10.	Appliquer le même signal/message d'auto surveillance pendant 401 ms une fois de plus que le nombre maximal de fois spécifié dans la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes de fraude en provenance de la même source doit être conforme à la CEI 62642-1, 8.10.
7	CIE en “mode en service”. NOTE Pour vérifier que si des signaux ou messages multiples d'auto surveillance sont appliqués, au moins un est traité correctement.	Appliquer des signaux ou des messages d'auto surveillance équivalant à 5 % de la capacité maximale des points d'alarme du CIE ou 5 (selon la valeur la plus importante) en 1 s.	Mesure générale	Au moins un signal ou message d'auto surveillance doit être traité conformément aux 8.4.1.2 et 8.9.
8	CIE en “mode en service” (avec plus d'une condition d'alarme contre la fraude)	Mettre hors service le CIE.	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.1.1.
9	CIE “en mode hors service”	Restaurer l'ensemble des conditions.	Mesure générale	Conformément au 8.3.5

11.4.4 Traitement des signaux ou des messages de défaut

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme aux 8.1.4, 8.3.5, 8.4.1, 8.5, 8.6, 8.9 et 8.10 et à recevoir, traiter, enregistrer et notifier un signal ou un message de défaut conformément aux exigences de la présente spécification. Les essais doivent être réalisés avec le CIE dans le mode en service et hors service afin de garantir que la détection des défauts satisfait à l'ensemble des exigences applicables.

b) Principe

Le principe consiste à démontrer la capacité du CIE à:

1) recevoir et traiter un signal ou un message de défaut conformément aux exigences relatives aux caractéristiques temporelles du traitement de la présente spécification, lorsque le CIE se trouve dans l'état en service et hors service;
2) fournir une ou des indication(s) et une ou des notification(s);
3) enregistrer correctement le ou les événement(s) dans le journal d'événements;
4) restaurer conformément au 8.3.5.

L'essai consiste à appliquer les conditions de défaut telles que spécifiées dans le 8.1.4 comme l'indique le Tableau 16.

Le système doit faire l'objet d'une surveillance afin de s'assurer que l'entrée a été traitée dans le délai requis et que l'enregistrement correct des événements, de la ou des notifications et des indications a été effectué.

Tableau 16 – Essai réalisé sur le traitement des signaux ou des messages de défaut

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous, avec toutes les entrées et sorties dans l'état normal.	Il convient d'appliquer un signal ou un message de défaut EPS uniquement lorsque cela est spécifié.	MESURE GENERALE Enregistrer l'état des indications et notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué. Moment où la notification intervient. Enregistrer le journal d'événements.	CRITERES GENERAUX Le traitement doit être réalisé conformément à la CEI 62642-1, Tableau 7 et 8.4.1. Les indications et notifications doivent être conformes à la CEI 62642-1, Tableaux 8, 9 et 10.
1	CIE en “mode en service”	Appliquer le signal ou le message de défaut pendant 10,1 s.	Mesure générale + Enregistrer l'identité du point d'alarme du défaut activé.	Critères généraux + La notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9. L'enregistrement doit être effectué conformément au 8.10.
2	CIE “en mode en service” (avec condition de défaut)	Mettre hors service le CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
3	CIE en “mode hors service”	Restaurer	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou des messages de défaut répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de défaut pendant 10,1 s une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes “défaut” enregistrées à partir de la même source doit être conforme à celui spécifié dans la CEI 62642-1, 8.10.
5	CIE “en mode hors service”	Appliquer le signal ou le message de défaut pendant 10,1 s.	Mesure générale	Critères généraux
6	CIE en “mode hors service”. NOTE Pour vérifier que les signaux ou messages de défaut répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de défaut pendant 10,1 s une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes “défaut” enregistrées à partir de la même source doit être conforme à celui spécifié dans la CEI 62642-1, 8.10.

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
7	CIE en “mode en service”. NOTE Pour vérifier que si des signaux ou messages de défaut répétitifs sont appliqués, au moins un est traité correctement.	Appliquer 5 signaux ou messages de défaut (ou le nombre maximal possible que l'EUT peut reconnaître si moins de 5) en 1 s.	Mesure générale	Au moins un signal ou message de défaut doit être traité conformément aux 8.4.1.2 et 8.9.
8	CIE en “mode en service” (avec plus d'une condition de défaut)	Mettre hors service CIE	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
9	CIE en “mode mise hors service”	Restaurer l'ensemble des conditions.	Mesure générale	Conformément au 8.3.5
10	CIE en “mode en service”	Appliquer au moins un de chacun des signaux ou messages de défaut, d'auto surveillance, d'alarme contre les hold-up et d'intrusion équivalant à 5 % de la capacité maximale des points d'alarme du CIE ou 5 (selon la valeur la plus importante) en 1 s.	Mesure générale + Enregistrer l'identité des points de défaut, d'auto surveillance, d'alarme contre les hold-up et d'intrusion activés.	Critères généraux + Il convient que la notification soit conforme au 8.4.1. Toutes les conditions doivent être correctement identifiées et enregistrées dans le journal d'événements au bon moment.
11	CIE en mode “hors service” Activer le retard de notification de défaut EPS requis par le 8.6.	Appliquer un signal ou un message de “défaut EPS”.	Mesure générale	La notification du défaut doit être retardée comme spécifié dans le 8.6.
12	Comme l'étape 11, lors du retard	Supprimer le signal ou le message de “défaut de l'EPS”.	Mesure générale	La notification doit être annulée conformément au 8.6.

11.4.5 Traitement des signaux ou des messages de masquage

a) Objet de l'essai

L'essai a pour objectif de démontrer la capacité du CIE à être conforme aux 8.1.6, 8.3.5, 8.5, 8.6, 8.9 et 8.10 et à recevoir, traiter, enregistrer et notifier un signal ou un message de masquage conformément aux exigences de la présente norme. Les essais doivent être réalisés avec le CIE dans les modes en service et hors service afin de garantir que la détection des défauts satisfait à l'ensemble des exigences applicables.

b) Principe

Cet essais doit être conduit comme suit:

1) recevoir et traiter un signal ou un message de masquage comme requis par les 8.1.6 et 8.10;
2) fournir une notification et une ou des indication(s);
3) enregistrer correctement le ou les événement(s) dans le journal d'événements.

L'essai consiste à appliquer des signaux ou des messages de masquage comme le spécifie le 8.1.6 et à vérifier que l'indication ou les indications et la notification ou les notifications sont correctes, se reporter au Tableau 17.

Tableau 17 – Essai réalisé sur le traitement des signaux ou des messages de masquage

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous, avec toutes les entrées et sorties dans l'état normal.	* Lors d'un traitement comme “intrusion”. Si traitement comme “ défaut “, remplacer par “10,1 s”.	MESURE GENERALE Enregistrer l'état des indications et notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué Moment où la notification intervient Enregistrer le journal d'événements.	CRITERES GENERAUX Le traitement doit être réalisé conformément à la CEI 62642-1, 8.4.5. Les indications et notifications doivent être conformes à la CEI 62642-1, Tableaux 8 et 9. NOTE La CEI 62642-1 permet de traiter les événements de masquage soit comme des “défauts” soit comme une réponse à une “intrusion”.
1	CIE en “mode en service”	Appliquer le signal ou le message de masquage pendant 401 ms *	Mesure générale Enregistrer l'identité du dispositif activé.	Critères généraux La notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9. L’enregistrement doit être effectué conformément au 8.10.
2	CIE “en mode en service” (avec condition de masquage)	Mettre hors service le CIE.	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
3	CIE en “mode hors service”	Restaurer.	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou des messages de masquage répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de masquage pendant 401 ms * une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes pour masquage enregistrées à partir de la même source doit être conforme à celui spécifié dans la CEI 62642-1, 8.10.
5	CIE “en mode hors service”	Appliquer le signal ou le message de masquage pendant 401 ms *.	Mesure générale	Critères généraux

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en “mode hors service”. NOTE Pour vérifier que des signaux ou des messages de masquage de défaut répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de masquage comme spécifié dans le 8.9 une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes pour masquage enregistré à partir de la même source doit être conforme à celui spécifié dans la CEI 62642-1, 8.10.
7	CIE en “mode en service”. NOTE Pour vérifier que si des signaux ou messages de masquage répétitifs sont appliqués, au moins un est traité correctement.	Appliquer 5 signaux ou messages de masquage (ou le nombre maximal possible que l'EUT peut reconnaître si moins de 5) en 1 s.	Mesure générale	Au moins un signal ou message de masquage doit être traité conformément aux 8.4.1.2 et 8.9.
* Lors d'un traitement comme “intrusion”. Si traitement comme “ défaut “, remplacer par “10,1 s”.				

11.4.6 Traitement des signaux ou des messages de réduction de la plage de détection

a) Objet de l’essai

L’essai a pour objet de démontrer la capacité du CIE à être conforme aux 8.1.7, 8.3.5, 8.5, 8.6, 8.9 et 8.10 et à recevoir, traiter, enregistrer et notifier un signal ou un message de réduction de la plage de détection conformément aux exigences de la présente norme. Les essais doivent être réalisés avec le CIE dans les modes en service et hors service afin de garantir que la détection des défauts satisfait à l’ensemble des exigences applicables.

b) Principe

Cet essais doit être conduit comme suit:

1) recevoir et traiter un signal ou un message de masquage comme requis par les 8.1.7 et 8.10;
2) fournir une notification et une ou des indication(s);
3) enregistrer correctement le ou les événement(s) dans le journal d’événements.

L’essai consiste à appliquer des signaux ou des messages de réduction de la plage de détection comme spécifié dans le 8.1.7 et à vérifier que l'indication et la notification ou les notifications sont correctes, se reporter au Tableau 18.

Tableau 18 – Essai réalisé sur le traitement des signaux ou des messages de réduction de la plage de détection

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état décrit dans les étapes ci-dessous, avec toutes les entrées et sorties dans l'état normal	*Lors d'un traitement comme une “intrusion”. Si traitement comme un “défaut”, remplacer par “10,1 s”.	MESURE GENERALE Enregistrer l'état des indications et notifications du CIE, ainsi que de tout dispositif d'entrée pour l'utilisateur associé (par exemple: claviers numériques distants). Moment où le signal/message est appliqué. Moment où la notification intervient. Enregistrer le journal d'événements	CRITERES GENERAUX Le traitement doit être réalisé conformément à la CEI 62642-1, 8.4.6. Les indications et notifications doivent être conformes à la CEI 62642-1, Tableaux 8, 9 et 10. NOTE La CEI 62642-1 permet de traiter les événements de réduction de la plage de détection SOIT comme des “défauts” soit comme une réponse à une “intrusion”.
1	CIE en “mode en service”	Appliquer le signal ou le message de réduction de la plage de détection pendant 401 ms *	Mesure générale Enregistrer l'identité du dispositif activé.	Critères généraux La notification doit intervenir dans le délai spécifié par la CEI 62642-1, 8.9. L’enregistrement doit être effectué conformément au 8.10.
2	CIE “en mode en service” (avec condition de réduction de la plage de détection)	Mettre hors service le CIE.	Mesure générale	Critères généraux Les indications doivent être conformes au 8.5.
3	CIE en “mode hors service”	Restaurer.	Mesure générale	Conformément au 8.3.5
4	CIE en “mode en service” NOTE Pour vérifier que des signaux ou des messages de réduction de la plage de détection répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de réduction de la plage de détection pendant 401 ms * une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes pour réduction de la plage de détection enregistrées à partir de la même source doit être comme spécifié dans la CEI 62642-1, 8.10.
5	CIE “mode hors service”	Appliquer le signal ou le message de réduction de la plage de détection pendant 401 ms *	Mesure générale	Critères généraux

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en “mode hors service”. NOTE Pour vérifier que des signaux ou des messages de réduction de la plage de détection répétitifs sont enregistrés dans le journal d'événements comme requis par la CEI 62642-1, 8.10.	Appliquer le même signal ou message de réduction de la plage de détection pendant 401 ms * une fois de plus que le maximum autorisé par la CEI 62642-1, 8.10. Ensuite, répéter l'étape 3.	Mesure générale	Le nombre d'alarmes pour réduction de la plage de détection enregistré à partir de la même source doit être comme spécifié dans la CEI 62642-1, 8.10.
7	CIE en “mode en service”. NOTE Pour vérifier que si des signaux ou messages de réduction de la plage de détection répétitifs sont appliqués, au moins un est traité correctement.	Appliquer 5 signaux ou messages de masquage, de réduction de la plage de détection (ou le nombre maximal possible que l'EUT peut reconnaître si moins de 5) en 1 s.	Mesure générale	Au moins un signal ou message de réduction de la plage de détection doit être traité conformément aux 8.4.1.2 et 8.9.
*Lors d'un traitement comme une “intrusion”. Si traitement comme un “défaut”, remplacer par “10,1 s”.				

11.4.7 Traitement du CIE en présence d'entrées non I&HAS

Traitement de signaux ou de messages obligatoires en présence de signaux ou de messages non I&HAS.

a) Objet de l’essai

L’objet de l’essai est de démontrer la capacité du CIE incluant des entrées à des fins autres que l'I&HAS à être conforme aux 8.1.8, 8.9 et 8.10; à recevoir et à traiter un signal ou un message de défaut, d’auto surveillance, d’alarme contre les hold-up et d’intrusion conformément aux exigences relatives aux caractéristiques temporelles du traitement de la présente spécification, lorsque le CIE se trouve dans les modes en service et hors service et que un ou plusieurs signaux ou messages facultatifs sont présents.

b) Principe

L'essai consiste à appliquer un signal ou un message obligatoire pendant qu'un signal ou un message d'un système autre que l'I&HAS est appliqué à une autre entrée du CIE et à surveiller que le signal ou le message obligatoire a été traité dans la période de temps requise ainsi que l'indication et la ou les notifications correctes ont lieu. Se reporter au Tableau 19.

Tableau 19 – Essai relatif au traitement du CIE en présence d'entrées d'un système autre que l'I&HAS

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	CIE en “mode hors service”	Appliquer un signal ou un message facultatif à l'entrée ou aux entrées du CIE. Dans les 500 ms suivant l'application du signal ou du message facultatif, appliquer un signal ou un message obligatoire à une entrée du CIE	Enregistrer: - l'état des sorties de notification - la période de temps entre l'entrée du signal ou du message obligatoire et le déclenchement de la notification obligatoire	La notification, résultant de l'entrée des signaux ou des messages obligatoires, doit être déclenchée dans le délai spécifié par la CEI 62642-1, 8.9.
2	CIE en “mode en service”	Répéter comme ci-dessus.	Comme ci-dessus	Comme ci-dessus

11.5 Niveau d'accès

11.5.1 Accès aux fonctions et commandes

a) Objet de l’essai

L’essai a pour objet de démontrer la capacité du CIE à être conforme aux 8.1.5, 8.3.1, 8.3.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.2 et 8.10, à fournir jusqu'à quatre niveaux d'accès et à vérifier la pertinence de l'accès aux fonctions et commandes.

b) Principe

L'essai consiste à tenter d'utiliser les fonctions et les commandes requises par les 8.1.5, 8.3.1, 8.3.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.2 et 8.10, en faisant fonctionner le CIE à chaque niveau d'accès et à vérifier que l'accès est accordé pour les fonctions autorisées et refusé pour les fonctions non autorisées (se reporter au Tableau 20).

Tableau 20 – Essai relatif à l'accès aux fonctions et commandes

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	Le CIE et tout ACE nécessaire doivent être montés conformément aux spécifications du fabricant.	Au niveau d'accès 1, tentative d'utilisation de l'ensemble des fonctions et commandes répertoriées aux 8.3.6, 8.3.7 et 8.3.9 de la CEI 62642-1 et dans la CEI 62642-1, Tableaux 2, 5, 6 et 8 et au 8.3.10.	Enregistrer si l'accès est autorisé.	L'accès est conforme au 8.3.9 et à la CEI 62642-1, Tableaux 2, 5, 6 et 8.
2	Comme ci-dessus	Répéter l'étape 1 pour le niveau d'accès 2.	Comme ci-dessus	Comme ci-dessus
3	Comme ci-dessus	Répéter l’étape 1 pour le niveau d'accès 3.	Comme ci-dessus Enregistrer si l'autorisation de niveau 2 pour un accès de niveau 3 est accordée “jusqu'à une suppression manuelle” ou “requise à chaque occasion”	Comme ci-dessus

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
4	Comme ci-dessus	Répéter l'étape 1 pour un niveau d'accès 4	Comme ci-dessus	Comme ci-dessus
NOTE Si un moyen est prévu pour avoir un accès de niveau 3 sans une autorisation de niveau 2 (se reporter à la CEI 62642-1, 8.3.1), non autorisé au grade 4:				
5	CIE hors service	Saisir la clé ou le code d'accès de niveau 3	Surveiller les sorties	Notifié par le WD interne (grades 2 et 3) à distance
6	Réaliser l'action définie par le fabricant pour réduire au silence le WD ou autoriser une temporisation, selon le cas	-	Surveiller les sorties et l'état.	WD réduit au silence. Accès de niveau 3 obtenu
7	CIE en service	Répéter les étapes 5 et 6	Surveiller les sorties et l'état.	Absence de réponse, reste à l'accès de niveau 1

11.6 Exigences relatives à l'autorisation

Lorsqu'un CIE peut accepter plus d'une méthode d'autorisation, le nombre de combinaisons doit faire l'objet d'une vérification individuelle pour chacune des méthodes conformément aux procédures suivantes afin de garantir la conformité si cette méthode uniquement est utilisée sur un système I&HAS.

11.6.1 Essais réalisés sur les clés mécaniques

a) Objet de l'essai

L'essai a pour objet de vérifier que les variantes de clés mécaniques, telles qu'elles sont spécifiées dans la CEI 62642-1, Tableau 3, sont satisfaites par le CIE et tout ACE associé et que les exigences des 8.3.2 et 8.3.2.1 sont satisfaites.

L'essai a pour objet de vérifier que la documentation du fabricant est conforme aux exigences de l'Article 9.

b) Principe

Le principe de l'essai consiste à vérifier que la plage de combinaisons de clés mécaniques est fournie et que les clés mécaniques invalides ne sont pas acceptées.

c) Conditions d'essai

Le fabricant doit fournir les informations suivantes au laboratoire d'essai:

1) nombre de variantes de clés;
2) méthode utilisée afin de déterminer le nombre de variantes de clés.

d) Procédure d'essai

L'essais doit être conduit comme suit:

1) Tenter de modifier l'état du CIE en utilisant une clé valide.
2) Tenter de modifier l'état du CIE en utilisant une clé invalide.
3) Examiner les informations du fabricant relatives à la construction de la clé et aux calculs.

e) Mesure

1) Vérifier que les informations et les calculs du fabricant sont valides.
Noter l'état du CIE avant et après utilisation d'une clé valide.
2) Noter l'état du CIE avant et après une tentative d'utilisation d'une clé invalide.
3) Enregistrer les détails relatifs aux clés invalides.

f) Critères de réussite/d'échec

1) La clé valide modifie l'état du CIE.
2) La clé invalide ne modifie pas l'état du CIE.
3) Les calculs et les informations fournis par le fabricant confirment que le nombre de combinaisons est conforme à la CEI 62642-1, Tableau 3.

11.6.2 Essais réalisés sur les clés logiques

Lorsqu'aucun essai spécifique n'est prévu pour le type de clé logique utilisé, il convient d'appliquer les principes de la “clé numérique”.

11.6.2.1 Essais réalisés sur les clés numériques

a) Objet de l’essai

L'essai a pour objet de vérifier que le nombre de variantes de clés logiques, telles qu'elles sont spécifiées dans la CEI 62642-1, Tableau 3, est satisfait par le CIE et tout ACE associé et que les exigences des 8.3.2 et 8.3.2.2.2 sont satisfaites.

L'essai a pour objet de vérifier que la documentation du fabricant est conforme aux exigences de l'Article 9.

b) Principe

Le principe de l'essai consiste à vérifier que la plage de variations de clés numériques est fournie, que les clés numériques invalides ne sont pas acceptées et que les exigences relatives au rejet de duplication et à l'alimentation sont satisfaites, si cela est applicable.

c) Conditions d’essai

Le fabricant doit fournir les informations suivantes au laboratoire d'essai:

1) Nombre de variantes de clés.
2) Méthode utilisée afin de déterminer le nombre de variantes de clés.
3) Si la plage opérationnelle de la clé numérique excède 1 m, méthode permettant de rejeter les copies non autorisées.

d) Procédure d’essai

1) Tenter de modifier l'état du CIE en utilisant une clé numérique valide.
2) Tenter de modifier l'état du CIE en utilisant une clé numérique non valide.
3) Examiner les informations du fabricant relatives à la construction de la clé numérique et aux calculs.
4) Vérifier le nombre de variations de la clé numérique.
5) Si la plage opérationnelle excède 1 m, soit
le fabricant doit fournir le moyen de simuler une clé dupliquée, soit
le fabricant doit fournir des détails relatifs au mode de fonctionnement du rejet de la copie.

6) Si celle-ci est auto-alimentée, le fabricant doit fournir le moyen de simuler une clé avec une faible charge du dispositif de stockage, comme requis par l'EN 50131-6, 7.7.4.1.

e) Mesure

1) Vérifier que les informations et les calculs du fabricant sont valides.
2) Noter l'état du CIE avant et après utilisation d'une clé numérique valide.
3) Noter l'état du CIE avant et après une tentative d'utilisation d'une clé numérique invalide.
4) Enregistrer les détails relatifs aux clés numériques invalides.
5) Enregistrer la plage de la clé numérique.
6) Enregistrer la réponse du système à une clé dupliquée, ou
Evaluer la technique de rejet de copie documentée du fabricant.
7) Enregistrer les réponses du système à une clé avec dispositif de stockage à faible tension.

f) Critères de réussite/d'échec

1) La clé numérique valide modifie l'état du CIE.
2) La clé numérique invalide ne modifie pas l'état du CIE.
3) Les calculs et les informations fournis par le fabricant confirment que le nombre de combinaisons est conforme à la CEI 62642-1, Tableau 3.
4) Si la plage excède 1 m, une clé dupliquée est rejetée, ou
la technique de protection contre la duplication du fabricant est conforme aux exigences relatives à la protection contre la duplication.
5) Si celle-ci est auto-alimentée, les exigences du 8.3.2.2.2 et de l'EN 50131-6, 7.7.4.1 pour les rapports avec une batterie faible sont satisfaites.

11.6.2.2 Essais réalisés sur les codes PIN

a) Objet de l'essai

L'essai a pour objet de vérifier que le nombre de combinaisons spécifiées dans le Tableau 3 de la CEI 62642-1 est satisfait par le CIE et tout ACE associé et que les exigences des 8.3.2 et 8.3.2.2.1 sont satisfaites.

L'essai a pour objet de vérifier que la documentation du fabricant est conforme aux exigences de l'Article 9.

b) Principe

Le principe de l'essai consiste à vérifier que la plage de variations de codes PIN est fournie et que les codes invalides ne sont pas acceptés.

c) Conditions d'essai

Aux fins de l'essai, le fabricant doit fournir les informations suivantes au laboratoire d'essai:

1) nombre de codes rejetés;
2) méthode utilisée afin de déterminer le nombre de variations;
3) pour chaque utilisateur, le nombre minimal de variantes de clés logiques doit être indiqué.

d) Procédure d'essai

1) Créer des échantillons de codes valides comme le décrit la documentation du CIE. Le nombre de codes valides à créer doit être le suivant: 10 pour le grade 1; 20 pour le grade 2; 50 pour le grade 3; 100 pour le grade 4.

2) Tenter de créer un code invalide.
3) Vérifier la validité des calculs du fabricant.

e) Mesure

1) Enregistrer les codes valides.
2) Enregistrer le code invalide.

f) Critères de réussite/d'échec

1) Tous les codes valides créés en "d) 1)" ci-dessus doivent être acceptés en fonction du grade.
2) Les codes invalides ne doivent pas être acceptés.
3) Les calculs doivent apparaître conformes aux combinaisons de code indiquées dans le Tableau 2.

11.6.2.3 Essais relatifs à une autorisation par des moyens biométriques

Les parties applicables de la procédure d'essai décrite pour les clés numériques au 11.6.2.1 doivent être appliquées.

De plus, le fabricant doit fournir des informations permettant au laboratoire d'essai d'évaluer la conformité aux exigences du 8.3.2.2.3 (Tableau 2).

11.6.2.4 Essais relatifs à une autorisation par une combinaison de clés

Lorsque des combinaisons de clés sont acceptées, comme spécifié au 8.3.2.4, chaque type doit être évalué comme étant approprié au type de clé. Les exigences temporelles du Tableau 3 doivent être satisfaites. Le nombre de combinaisons de chaque type doit être multiplié pour évaluer la conformité à la CEI 62642-1, Tableau 3.

11.6.3 Tentatives d'autorisation invalide

a) Objet de l'essai

L'essai a pour objet de vérifier que la détection et la notification d'une tentative de saisie de clés logiques (lorsque le CIE dispose du moyen de les distinguer) ou de clés mécaniques invalides sont conformes au 8.3.2 et au Tableau 3.

b) Principe

L'essai consiste à saisir une série de clés logiques ou mécaniques (selon le cas) invalides et à déterminer que, lorsque le nombre de tentatives invalides a été effectué comme le spécifie le Tableau 3, le dispositif d'entrée pour l'utilisateur est désactivé et/ou un signal ou un message d'auto surveillance est généré et enregistré dans le journal d'événements comme spécifié. Se reporter aux Tableaux 21 et 22.

Lors d'un essai réalisé sur des codes PIN invalides, au moins une tentative doit prendre la forme d'une saisie de code valide non achevée dans les 60 s.

Tableau 21 – Essai relatif à la désactivation d'un dispositif d'entrée pour l'utilisateur par des clés invalides

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
Répéter pour chaque type de tentative invalide – c'est-à-dire le code PIN, la clé numérique, la clé biométrique et (si le CIE dispose du moyen lui permettant de la détecter) la clé mécanique				
Si le CIE dispose du moyen de désactiver le dispositif d'entrée pour l'utilisateur, réaliser cette série d'essais				
	GENERAL: Le CIE doit être configuré avec ses entrées et ses sorties dans leur état normal permettant la mise en service du CIE et la génération d'alarmes à partir d'au moins 1 point d'alarme.	GENERAL: Les étapes 2, 4, 5, 6 et 7 doivent être répétées dans le mode “HORS SERVICE” du CIE.		
1	CIE hors service	Saisir une clé valide et tenter de mettre en service le CIE.	Enregistrer l'état du CIE.	CIE en service
2	CIE en service	Saisir une série de clés invalides conformément au Tableau 1 afin de tenter de désactiver initialement le dispositif d'entrée pour l'utilisateur.	Enregistrer l'état du CIE, désactivation du dispositif d'entrée pour l'utilisateur, conditions de fraude et journal d'événements.	Il convient que le CIE ne change pas d'état, le dispositif d'entrée pour l'utilisateur doit être désactivé, la génération de conditions de fraude et le journal d'événements doit être conforme au Tableau 1.
3	CIE en service	Durant la “période de désactivation” appliquer un signal ou un message d'alarme.	Enregistrer si la condition d'alarme est traitée.	L'alarme générée durant la période de désactivation doit être traitée conformément à la CEI 62642-1, Tableau 7 et 8.4.1.
4	CIE en service	Durant la “période de désactivation”, tenter de saisir une clé valide.	Enregistrer si le dispositif d'entrée pour l'utilisateur répond à l'opération.	Le CIE ne doit pas changer d'état. Le dispositif d'entrée pour l'utilisateur doit demeurer désactivé.
5	CIE en service	Lorsque la période de désactivation a expiré, saisir une autre série de clés invalides conformément au Tableau 4.	Enregistrer l'état du CIE, désactivation du dispositif d'entrée pour l'utilisateur, conditions de fraude et journal d'événements.	Le CIE ne doit pas changer d'état et doit être conforme au Tableau 4.
6	CIE en service	Durant la “période de désactivation” tenter de saisir une clé valide.	Enregistrer si le dispositif d'entrée pour l'utilisateur est disponible.	Le CIE ne doit pas changer d'état Le dispositif d'entrée pour l'utilisateur doit rester désactivé.
7	CIE en service	Lorsque la période de désactivation a expiré, saisir une clé valide et tenter de modifier l'état du CIE.	Enregistrer l'état du CIE.	Le CIE doit changer d'état.

Tableau 22 – Essai relatif à la génération d'un signal ou d'un message d'auto surveillance par des clés invalides

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
Si le CIE est doté du dispositif conformément au Tableau 1 lui permettant de générer un signal ou un message d'auto surveillance, réaliser cette série d'essais				
	GENERAL: Le CIE doit être configuré avec ses entrées et ses sorties dans leur état normal permettant la mise en service du CIE et la génération d'alarmes à partir d'au moins 1 point d'alarme.	GENERAL: Les étapes 2 et 3 doivent être répétées dans le mode "HORS SERVICE" du CIE.		
1	CIE hors service	Saisir une clé valide et tenter de mettre en service le CIE.	Enregistrer l'état du CIE.	CIE en service
2	CIE en service	Saisir une série de clés invalides conformément au Tableau 4 afin de tenter de générer une condition de fraude.	Enregistrer l'état du CIE, conditions de fraude et journal d'événements.	Le CIE ne doit pas changer d'état, la génération de conditions de fraude et le journal d'événements doivent être conformes au Tableau 1.
3	CIE en service	Saisir une clé valide pour valider la condition de fraude.	Enregistrer l'état du CIE, conditions de fraude et journal d'événements.	La condition de fraude doit être validée et doit être conforme au Tableau 1.

11.7 Essais opérationnels

11.7.1 Procédures de mise en service

a) Objet de l'essai

L'objet de l'essai est de vérifier que toutes les procédures de mise en service sont conformes aux 8.3.3, 8.3.3.2 et 8.3.3.3.

b) Principe

L'essai consiste à mettre en service le CIE et à vérifier que les procédures sont conformes aux exigences de la présente norme (voir Tableau 23).

Tableau 23 – Essai relatif à la procédure de mise en service

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état “hors service”. Pour les besoins de cette série d'essais, les clés et/ou codes doivent être sélectionnés pour disposer des autorisations nécessaires pour les fonctions d'“inhibition” et d'“annulation”.		GENERAL: Enregistrer l'état du CIE	CRITERES GENERAUX Lorsque la mise en service du CIE échoue, des moyens doivent être prévus pour l'indiquer ou le notifier. Si l'indication de l'état de mise en service est fournie, celle-ci doit être limitée dans le temps conformément à la CEI 62642-1, 8.3.7. L'enregistrement doit être conforme au 8.10.
Réaliser la série d'essais suivante pour chaque méthode de mise en service indiquée dans la documentation du fabricant.				
1	Le CIE est hors service	Lancer la procédure de sortie.	Enregistrer l'état du CIE.	Le CIE doit se mettre en service et donner des indications en conséquence
2	CIE hors service	La procédure de mise en service est déclenchée mais n'a pas pu arriver à son terme. La temporisation “Echec de mise en service” expire.	Enregistrer l'état du CIE.	Condition de sortie incomplète indiquée et/ou notifiée, conformément au 8.3.3.3 CIE non passé en service Absence de notification d'alarme
Pour un CIE dans lequel une mise en service en utilisant une fonction de dernière issue est possible, vérifier qu'il existe un moyen permettant de sélectionner les points d'alarme à inclure dans la fonction de dernière issue et:				
3	CIE hors service	Lancer la procédure de mise en service (temporisation de sortie).	Enregistrer l'état du CIE.	La procédure de mise en service doit être lancée et indiquée conformément au 8.3.3.2 et à la CEI 62642-1, Tableaux 8 et 9.
4		Activer un point d'alarme de la fonction de dernière issue durant la période de sortie.	Enregistrer l'état du CIE.	Le point d'alarme activé ne doit pas provoquer de notification d'alarme.
5		S'assurer que le point d'alarme ne se trouve plus dans l'état activé. Laisser s'achever la procédure de mise en service ou achever la procédure de mise en service selon la méthode.	Enregistrer l'état du CIE.	La procédure de mise en service doit être achevée. Le CIE est en service, conformément au 8.3.3.2.
6	CIE hors service Procédure de sortie déclenchée Point d'alarme du chemin d'accès activé	Le point d'alarme du chemin d'accès reste activé La temporisation de sortie ou la temporisation «Echec de mise en service” expire	Enregistrer l'état du CIE.	Condition de sortie incomplète indiquée et/ou notifiée conformément au 8.3.3.3 CIE non passé en service Absence de notification d'alarme

Pour un CIE incluant un dispositif de mise en service par un accès de niveau 1 comme l'autorise la CEI 62642-1, 8.3.4 (grade 1 uniquement):				
7	CIE hors service	Lancer une mise en service par une action de niveau 1 conformément aux instructions du fabricant.	Enregistrer l'action du CIE.	Le CIE doit entamer la procédure de mise en service.
8	Durant la procédure de mise en service	Activer une fonction, conformément aux instructions du fabricant, “d’annulation de la mise en service” par une action de niveau 1.	Enregistrer l'action du CIE	Le CIE doit annuler la procédure de mise en service et rester hors service.
9	CIE hors service	Lancer une mise en service par une action de niveau 2 conformément aux instructions du fabricant.	Enregistrer l'action du CIE	Le CIE doit entamer la procédure de mise en service.
10	Durant la procédure de mise en service	Activer une fonction conformément aux instructions du fabricant, “d’annulation de la mise en service” par une action de niveau 1.	Enregistrer l'action du CIE	Le CIE doit poursuivre la procédure de mise en service. Autoriser la mise en service.
11	CIE en service	Activer une fonction conformément aux instructions du fabricant, “d’annulation de la mise en service” par une action de niveau 1.	Enregistrer l'action du CIE	Le CIE doit rester en service.

11.7.2 Interdiction de la mise en service et annulation de l'interdiction des procédures de mise en service

a) Objet de l'essai

L'essai a pour objet de vérifier que toutes les procédures sont conformes au 8.3.3.1.

b) Principe

L'essai consiste à tenter de mettre en service le CIE et à vérifier que toutes les réponses sont conformes aux exigences de la présente norme (voir Tableau 24).

Tableau 24 – Essai relatif à l'interdiction de la mise en service et à l'annulation de l'interdiction de la procédure de mise en service

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état “hors service”. Pour les besoins de cette série d'essais, les clés et/ou codes doivent être sélectionnés pour disposer des autorisations nécessaires pour les fonctions d'“inhibition” et d'“annulation”.	La mise à disposition d'une fonction d'annulation de l'interdiction de la mise en service et d'une fonction d'inhibition décrites dans l'essai n'est pas obligatoire (8.3.3.1 et 8.3.6).	GENERAL: Enregistrer l'état du CIE.	CRITERES GENERAUX Lorsque la mise en service du CIE échoue, des moyens doivent être prévus pour l'indiquer ou le notifier. Si l'indication de l'état de mise en service est fournie, celle-ci doit être limitée dans le temps conformément à la CEI 62642-1, 8.3.7. L'enregistrement doit être conforme au 8.10.
Réaliser la série suivante d'essais pour chaque méthode de mise en service indiquée dans la documentation du fabricant et pour chaque condition spécifiée dans la CEI 62642-1, Tableau 4.				
1	Point d'alarme (non alloué à une fonction de dernière issue) dans l'état actif CIE hors service	Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit être conforme au 8.3.3 et à la CEI 62642-1, Tableau 4.
2	Point d'alarme (non alloué à une fonction de dernière issue) dans l'état actif. Mise en service interdite (voir étape 1) CIE hors service	Inhiber le point d'alarme actif (si la fonction est fournie) – voir le 8.3.6. Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit se poursuivre conformément à la CEI 62642-1, Tableau 4 et s'achever conformément aux instructions du fabricant.
3	CIE dans l'état “hors service”. Signal ou message d'auto surveillance appliqué au CIE	Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit être interdite conformément à la CEI 62642-1, Tableau 4
4	Mise en service interdite (voir étape 3) CIE hors service	Annuler le signal ou le message d'auto surveillance (si la fonction est fournie) – voir la CEI 62642-1, Tableau 5 Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit se poursuivre conformément à la CEI 62642-1, Tableau 4 et s'achever conformément aux instructions du fabricant.
5	Le CIE se trouve dans l'état “hors service”. Signal ou message d'alarme contre les hold-up appliqué au CIE	Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit être interdite conformément à la CEI 62642-1, Tableau 4.
6	Mise en service interdite (voir étape 5) CIE hors service	Inhiber le dispositif d'alarme contre les hold-up (si la fonction est fournie) – voir le 8.3.6. Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit se poursuivre conformément à la CEI 62642-1, Tableau 4 et s'achever conformément aux instructions du fabricant.
Pour le masquage du détecteur de mouvements, la réduction de la plage de détection du détecteur de mouvements et chaque signal ou message de défaut spécifiés dans la CEI 62642-1, Tableau 4, répéter les étapes 7 et 8.				

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
7	Le CIE se trouve dans l'état “hors service”. Appliquer le signal ou le message de défaut au CIE.	Tenter de mettre en service le système.	Enregistrer l'état du CIE.	La procédure de mise en service doit être interdite conformément à la CEI 62642-1, Tableau 4.
8	Mise en service interdite (voir étape 7) CIE hors service	Annuler l'interdiction de mise en service (si la fonction est fournie) – voir le 8.3.6.	Enregistrer l'état du CIE.	La procédure de mise en service doit se poursuivre conformément à la CEI 62642-1, Tableau 4 et s'achever selon les instructions du fabricant.

11.7.3 Etat en service

Avant de soumettre à essai les fonctions de mise hors service, déterminer la ou les option(s) pour l'état en service fournie(s) à partir de la documentation du fabricant (voir le 8.3.3.4).

Au moins une des options décrites dans la CEI 62642-1, 8.3.7 doit être fournie, selon le grade de sécurité.

Selon la ou les option(s) fournie(s), la ou les partie(s) applicable(s) du 11.7.4 doivent faire l'objet d'un essai.

11.7.4 Procédures de mise hors service

a) Objet de l'essai

L'essai a pour objet de vérifier que toutes les procédures sont conformes aux exigences du 8.3.4.

b) Principe

L'essai consiste à mettre hors service le CIE en utilisant toutes les procédures fournies comme le spécifie la documentation du fabricant et à vérifier que celles-ci sont conformes aux exigences contenues dans la présente spécification (voir Tableau 25).

Tableau 25 – Essai relatif à la procédure de mise hors service

Etape	Condition d'essai (c)	Procédure (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état "en service". Les clés ainsi que les codes utilisés sont tous valides par rapport à l'autorité nécessaire.		GENERAL: Enregistrer l'état du CIE.	CRITERES GENERAUX L'indication de l'état hors service doit être limitée dans le temps conformément à la CEI 62642-1, 8.3.8.2. L'enregistrement doit être conforme au 8.10.
Réaliser la série d'essais suivante pour chaque méthode de mise hors service indiquée dans la documentation du fabricant.				
1	CIE en service, dans un état normal sans activation d'alarmes ou de signaux et messages d'auto surveillance.	Tenter de mettre hors service manuellement le système.	Enregistrer l'état du CIE.	La procédure de mise hors service doit s'achever.
2	CIE en service Point d'alarme (non une fonction de première issue convenue) dans l'état actif	Tenter de mettre hors service manuellement le système.	Enregistrer l'état du CIE.	La procédure de mise hors service doit s'achever. La notification, l'indication et l'enregistrement des événements doivent être conformes à la CEI 62642-1, Tableaux 7, 8, 9 et 22.
Pour un CIE disposant d'une fonction de première issue, réaliser la série d'essais suivante pour chaque méthode de mise hors service indiquée dans la documentation du fabricant.				
3	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE. Enregistrer l'indication.	La procédure de mise hors service doit être lancée. L'indication doit être conforme à la CEI 62642-1, 8.3.8.2 et aux Tableaux 8 et 9 et enregistrée dans le journal d'événements conformément à la CEI 62642-1, Tableau 22.
4	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE.	La procédure de mise hors service doit être lancée.
5		Générer une alarme d'intrusion à partir d'un point d'alarme de la fonction de première issue.	Enregistrer l'état du CIE.	Une alarme d'intrusion ne doit pas être notifiée.
6		Ne pas achever la procédure de mise hors service (laisser la temporisation d'entrée expirer).	Enregistrer l'état du CIE.	Une condition d'alarme doit être notifiée conformément à la CEI 62642-1, 8.3.8.2.
7	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE. Enregistrer l'indication.	La procédure de mise hors service doit être lancée. L'indication doit être conforme à la CEI 62642-1, 8.3.8.2 et aux Tableaux 8 et 9.

Etape	Condition d'essai (c)	Procédure (d)	Mesure (e)	Critères de réussite/d'échec (f)
8	Procédure de mise hors service en cours	Générer une alarme d'intrusion à partir d'un point d'alarme de la fonction de première issue et achever la procédure d'entrée.	Enregistrer l'état du CIE Enregistrer l'indication et la notification	Le CIE est hors service. L'alarme d'intrusion ne doit pas être traitée. Une procédure correcte d'entrée doit être indiquée selon la CEI 62642-1, 8.3.8.2 et les Tableaux 8 et 9 et enregistrée dans le journal d'événements conformément à la CEI 62642-1, Tableau 22.
9	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE.	La procédure de mise hors service doit être lancée.
10		Générer une alarme de fraude à partir d'un point d'alarme de fonction de première issue.	Enregistrer l'état du CIE.	L'alarme de fraude doit être notifiée.
11	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE.	La procédure de mise hors service doit être lancée.
12		Générer une alarme d'intrusion à partir d'un point d'alarme autre que de la fonction de première issue.	Enregistrer l'état du CIE.	L'indication ou le dispositif d'avertissement doit être activé conformément à la CEI 62642-1, 8.3.8.2.
13	La mise hors service est en cours	Attendre l'arrivée à expiration de la temporisation programmée ou spécifiée par le fabricant après indication ou activation du WD interne. La temporisation MINIMALE est de 30 s	Enregistrer l'état du CIE.	Lorsque des dispositifs de notification à distance sont connectés, s'assurer de l'absence d'activation avant l'achèvement du délai requis par la CEI 62642-1, 8.3.8.2.
14	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE.	La procédure de mise hors service doit être lancée.
15		Ne pas achever la procédure de mise hors service (laisser la temporisation d'entrée arriver à expiration).	Enregistrer l'état du CIE.	L'alarme doit être notifiée conformément à la CEI 62642-1, 8.3.8.2.
16	CIE en service	Lancer manuellement la procédure de mise hors service (temporisation d'entrée).	Enregistrer l'état du CIE.	La procédure de mise hors service doit être lancée.

Etape	Condition d'essai (c)	Procédure (d)	Mesure (e)	Critères de réussite/d'échec (f)
17		Générer une alarme à partir d'un point d'alarme autre que de la fonction de première issue.	Enregistrer l'état du CIE.	L'indication ou le dispositif d'avertissement doit être activé conformément à la CEI 62642-1, 8.3.8.2.
18		Achever la procédure de mise hors service avant que le délai de notification ne vienne à expiration, voir l'alinéa 3 de la CEI 62642-1, 8.3.8.2.	Enregistrer l'état du CIE.	L'indicateur ou les dispositifs d'avertissement doivent être restaurés et une notification à distance ne doit pas avoir lieu. Le CIE doit être hors service.

11.7.5 Mise en service et/ou mise hors service automatique à des périodes prédéterminées

Si le CIE dispose d'une fonction de mise en service et/ou mise hors service automatique à des périodes prédéterminées, l'essai suivant doit s'appliquer:

a) Objet de l'essai

L'objet de l'essai est de vérifier que toutes les procédures sont conformes aux 8.3.3, 8.3.3.1 et 8.3.4.

b) Principe

L'essai consiste à tenter de mettre en service le CIE et à vérifier que les réponses sont conformes aux exigences de la présente norme (voir Tableau 26).

Tableau 26 – Essai relatif à la mise en service et/ou la mise hors service automatique à des périodes prédéterminées

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
	ETAT GENERAL Le CIE se trouve dans l'état “hors service”. Pour les besoins de cette série d'essais, les clés et/ou codes doivent être sélectionnés pour disposer des autorisations nécessaires pour les fonctions d'“inhibition” et d'“annulation”.	La fourniture d'une fonction d'annulation de l'interdiction de la mise en service et d'une fonction d'inhibition décrites dans l'essai n'est pas obligatoire (8.3.3.1 et 8.3.6).	GENERAL: Enregistrer l'état du CIE.	CRITERES GENERAUX Lorsque la mise en service du CIE échoue, des moyens doivent être prévus pour l'indiquer ou le notifier. Si l'indication de l'état de mise en service est fournie, celle-ci doit être limitée dans le temps conformément à la CEI 62642-1, 8.3.7. L'enregistrement doit être conforme au 8.10.
Si le CIE dispose d'une fonction de mise en service automatique:				
1	Le CIE est hors service, avant que l'indication de mise en service à une période prédéterminée ne soit programmée.	Autoriser une séquence automatique.	Surveiller les indications et l'état du CIE.	Indication de mise en service à une période prédéterminée disponible telle que documentée par le fabricant. La mise en service et l'annulation de l'interdiction de mise en service doivent être entrées dans le journal d'événements.
2	Le CIE étant en service, créer une alarme.	Autoriser une mise hors service automatique.	Surveiller l'état et les indications.	La mise hors service a lieu comme programmé. Présence d'une indication d'alerte. Mise hors service entrée dans le journal d'événements
3		Obtenir un accès de niveau 2.	Enregistrer les informations affichées.	Enregistrement correct de l'alarme créée dans l'état en service. L'alarme est présente dans le journal d'événements.
4	Le CIE est hors service, avant que l'indication de mise en service à une période prédéterminée ne soit programmée. Condition d'interdiction de la mise en service présente	Autoriser une séquence automatique.	Surveiller les indications et l'état du CIE.	Indication de mise en service à une période prédéterminée disponible telle que documentée par le fabricant. Mise en service interdite ou interdiction de mise en service automatiquement annulée. La mise en service et l'annulation de l'interdiction de la mise en service doivent être entrées dans le journal d'événements.
Si le CIE dispose d'une fonction de mise hors service automatique:				
5	CIE en service	Lancer la séquence de mise hors service conformément aux instructions du fabricant.	Enregistrer l'état du CIE.	La procédure de mise hors service doit s'achever.

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
6	CIE en service et dans la condition d'alarme	Lancer la séquence de mise hors service conformément aux instructions du fabricant	Enregistrer l'état du CIE.	La procédure de mise hors service doit s'achever. La condition d'alarme ne doit pas être annulée. L'événement d'alarme et la mise hors service doivent être entrés dans le journal d'événements.

11.7.6 Fonctions d'inhibition et d'isolement

a) Objet de l'essai

L'essai a pour objet de vérifier que les fonctions d'inhibition ou d'isolement sont conformes aux exigences des 8.3.6 et 8.3.7.

NOTE Ces essais ne s'appliquent que si une ou les deux fonctions sont prévues.

b) Principe

L'essai consiste à activer des modes d'inhibition et d'isolement afin de garantir une fonctionnalité correcte (voir Tableau 27).

c) Condition d'essai

Examiner la documentation du fabricant afin de confirmer des détails relatifs à la fonctionnalité.

L'essai doit être réalisé avec le système initialement dans l'état hors service.

Tableau 27 – Fonctions d'inhibition et d'isolement

	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f) NOTE La CEI 62642-1, Tableau 22 définit les informations du journal d'événements requises, ainsi que le grade correspondant.
FONCTION D'INHIBITION			
1	Mettre en service le système, en inhibant un point d'alarme comme le décrit le fabricant.		
2	Appliquer un signal ou un message à l'entrée inhibée pendant la durée minimale nécessaire au déclenchement, suivant le type.	Surveiller les sorties de notification.	Le journal d'événements doit enregistrer l'inhibition. Il ne doit y avoir ni notification ni événement du journal pour une condition d'alarme.
3	Mettre hors service le système puis le remettre en service.		
4	Appliquer un signal ou un message à l'entrée inhibée auparavant pendant la durée minimale nécessaire au déclenchement, selon le type.	Surveiller les sorties de notification.	La notification et le journal d'événements doivent faire état d'une réponse normale (non inhibée).
5	Répéter les étapes en utilisant un point d'alarme contre les hold-up	Surveiller les réponses du système.	Il ne doit pas être possible d'inhiber un point d'alarme contre les hold-up.
FONCTION D'ISOLEMENT			
6	Isoler un point d'alarme comme le décrit le fabricant.		L'isolement ne doit être possible qu'au niveau ou niveau(x) d'accès spécifié(s). Le journal d'événements doit enregistrer l'isolement.
7	Mettre en service le système I&HAS.		
8	Appliquer un signal ou un message à une entrée isolée pendant la durée minimale nécessaire au déclenchement, suivant le type.	Surveiller les réponses du système.	Il ne doit pas y avoir de notification ou d'événement de journal pour une condition d'alarme.
9	Mettre hors service le système puis le remettre en service.		
10	Répéter l'étape 8.	Surveiller les réponses du système.	Il ne doit pas y avoir de notification ou d'événement de journal pour une condition d'alarme.
11	Rétablir le point d'alarme comme le décrit le fabricant.		Cette opération ne doit être possible qu'au niveau ou niveau(x) d'accès spécifié(s).
12	Répéter l'étape 8.	Surveiller les réponses du système.	La notification et le journal d'événements doivent faire état d'une réponse normale (rétabli).

11.7.7 Fonctions d'essai

a) Objet de l'essai

L'essai a pour objet de vérifier la capacité du CIE à autoriser la réalisation de fonctions d'essai conformément aux exigences des 8.3.8, 8.3.9 et 8.10.

b) Principe

L'essai consiste à activer les modes d'essai afin de garantir une fonctionnalité correcte (voir Tableau 28).

c) Condition d'essai

L'essai doit être réalisé avec le système initialement dans l'état hors service.

Tableau 28 – Vérification des fonctions d'essai

	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	Le système étant hors service et dans l'état normal, utiliser un moyen d'accès de niveau 2 afin d'entrer dans le mode d'essai de détection (8.3.8).	Appliquer au moins 5 signaux ou messages d'intrusion comme le spécifie le 8.9. Enregistrer l'identité des points d'alarme activés.	Le CIE doit fournir un moyen permettant de confirmer que chacune des activations a été détectée.
Si le CIE inclut une fonction "essai d'inhibition" (8.3.9)			
2	Utiliser un moyen d'accès de niveau 3 afin de soumettre au moins 2 points d'alarme à l'essai d'inhibition.	Enregistrer les points d'alarme ainsi programmes et, lorsque la suppression est automatique, la période de temps pour l'essai.	
3	Mettre en service le CIE.	Enregistrer les indications au cours de la procédure de mise en service.	Au cours de la procédure de mise en service, une indication doit être fournie selon laquelle les points d'alarme font l'objet d'un essai d'inhibition conformément au 8.3.9.
4	Pendant que le CIE est en service, activer les points d'alarme qui font l'objet de l'essai.	Enregistrer l'identité des points d'alarme activés et l'état des sorties de notification et indication du CIE.	Les activations ne doivent pas être notifiées.
5	Mettre hors service le CIE.	Enregistrer l'état des sorties d'indication ainsi que les journaux d'événements.	Les activations doivent être indiquées au moment de la mise hors service conformément au 8.5. L'enregistrement doit être conforme aux 8.3.9 et 8.10.
6	Lorsque la sortie du mode d'essai est automatique:	Répéter les étapes 3 et 4 un jour avant que la période d'essai ne doive se terminer.	L'essai doit rester actif.
7		Répéter les étapes 3 et 4 après que la période d'essai ne doive arriver à expiration.	Il ne doit y avoir aucune indication à l'étape 3; une alarme doit être notifiée et indiquée à l'étape 4.
8	Lorsque la sortie du mode d'essai n'est pas automatique:	Utiliser un moyen d'accès de niveau 3 pour ne plus soumettre les points d'alarme à l'essai d'immersion.	

11.7.8 Autres fonctions

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à fonctionner normalement pendant qu'une fonction non prévue dans la CEI 62642-1 est utilisée comme requis par le 8.3.10.

b) Principe

L'essai consiste à activer une fonction supplémentaire lors du fonctionnement normal du CIE et à vérifier que la conformité à la présente norme n'est pas affectée.

Le fabricant doit indiquer les fonctions supplémentaires fournies, leur mode d'activation et les fonctions du système I&HAS pouvant être gênées par ces fonctions supplémentaires.

c) Condition d'essai

Le CIE doit se trouver dans l'état adapté à l'essai de la fonction du système I&HAS identifiée.

d) Procédure

Activer les fonctions du système I&HAS et les fonctions supplémentaires simultanément (ou dans un délai convenu).

e) Mesure

Surveiller l'activation de la fonction du système I&HAS.

f) Critères de réussite/d'échec

L'activation de la fonction du système I&HAS doit être conforme aux exigences de la présente norme.

11.7.9 Surveillance du traitement du CIE

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE comportant un traitement de données sérielles commandé par un programme à être conforme au 8.4.3 afin de détecter et de réagir à des défauts de traitement.

b) Principe

L'essai consiste à introduire un défaut de traitement et à surveiller que la ou les bonne(s) indication(s) et notification(s) se produisent, voir Tableau 29.

Le fabricant doit indiquer le mode d'introduction d'un défaut de traitement à des fins d'essai.

Tableau 29 – Essai relatif à la surveillance du traitement du CIE

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	Le CIE doit se trouver en mode hors service, avec toutes les entrées et les sorties dans l'état normal.	Introduire un défaut de la fonction de traitement.	Enregistrer l'état de la sortie de supervision du traitement.	Pour les grades 3 et 4, la sortie doit changer d'état dans les 40 s à moins que le CIE n'ait redémarré avec succès plus tôt.
2		Sortir du mode de défaut et appliquer l'essai fonctionnel réduit.	Enregistrer l'état du CIE, le journal d'événements ainsi que les indications.	Pour les grades 3 et 4, si la tentative de redémarrage du processeur réussit, le CIE doit redémarrer dans son mode de fonctionnement antérieur, l'essai fonctionnel réduit doit s'achever avec succès et un défaut du CIE doit être indiqué et enregistré dans le journal d'événements.
3	Répéter les étapes 1 et 2 comme ci-dessus pour le "mode en service".	Répéter comme ci-dessus.	Comme ci-dessus.	Comme ci-dessus.

11.7.10 Disponibilité des indications

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme aux exigences du 8.5.1.

b) Principe

L'essai consiste à introduire une condition nécessitant une indication obligatoire et à s'assurer que les exigences de la CEI 62642-1, 8.5.2 et 8.5.3 sont satisfaites, conformément au Tableau 30.

Tableau 30 – Essai relatif à la disponibilité des indications

Etape	Condition d'essai (c)	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	Le CIE doit se trouver dans le mode hors service, avec toutes les entrées et sorties dans l'état normal.	Introduire un défaut nécessitant une indication obligatoire conformément à la CEI 62642-1, Tableau 8.	Enregistrer les indications.	Présence d'une indication d'alerte
2	Avoir accès au CIE au niveau 2.	Visualiser les informations affichées.	Enregistrer les indications.	Indication correcte de la condition de défaut générée.
3	Revenir à un accès de niveau 1 conformément aux spécifications du fabricant – en utilisant une réponse automatique (temporisée) si celle-ci est fournie.	Visualiser les informations affichées.	Enregistrer les indications.	Présence d'une indication d'alerte. Si action automatique (temporisée), celle-ci est réalisée dans le délai spécifié par le fabricant.
4	Supprimer la condition de défaut appliquée à l'étape 1.	Visualiser les informations affichées.	Enregistrer les indications.	Présence d'une indication d'alerte.
5	Avoir accès au CIE au niveau 2.	Visualiser les informations affichées.	Enregistrer les indications.	L'indication de la condition de défaut reste disponible.
6	Revenir à un niveau d'accès 1 et restaurer.	Visualiser les informations affichées.	Enregistrer les indications.	Absence d'indication

11.8 Essais relatifs à la sécurité contre la fraude

11.8.1 ACE de type A

La documentation fournie par le fabricant venant à l'appui d'une revendication de statut d'un ACE “type A” doit être vérifiée.

11.8.2 Protection contre la fraude

a) Principe

Le principe de cet essai consiste à faire appel à des essais de choc afin de vérifier que le boîtier du CIE/de l'ACE satisfait aux exigences en matière de protection contre la fraude conformément au 8.7.1.

b) Procédure

Soumettre le boîtier du CIE/de l'ACE à des essais de choc en utilisant la méthodologie de la CEI 62599-1, avec un équipement satisfaisant aux exigences de la CEI 60068-2-75:1997 aux niveaux de sévérité spécifiés dans le 8.7.1.

c) Mesure

Evaluer l'EUT comme le décrit l'essai fonctionnel réduit du 11.3.

d) Critères de réussite/d'échec

L'EUT doit satisfaire aux exigences de l'essai fonctionnel réduit avant, pendant et après l'essai.

La génération de signaux ou de messages est autorisée suite à cet essai.

Il ne doit y avoir aucun signe de détérioration mécanique autorisant un accès aux éléments internes du boîtier du CIE/de l'ACE à moins qu'un signal ou un message d'auto surveillance n'ait été généré.

Il ne doit y avoir aucune détérioration du boîtier de l'ACE autorisant une modification de l'état du système I&HAS ou empêchant le CIE de déclencher toutes les réponses de notification obligatoires.

11.8.3 Détection de la fraude – Accès à l'intérieur du boîtier

a) Principe

Le principe de cet essai consiste à vérifier qu'il est impossible d'introduire un outil dans le CIE/l'ACE dans sa position normale de montage et d'entraver le fonctionnement des circuits de détection de la fraude avant qu'un signal ou un message d'auto surveillance ne soit généré (voir le 8.7.2.1).

b) Conditions d'essai

Il convient que le CIE se trouve dans l'état hors service.

c) Montage

Monter le CIE/l'ACE conformément aux instructions du fabricant avec le boîtier solidement fermé.

d) Procédure

Ouvrir le boîtier du CIE/de l'ACE normalement et tenter d'introduire un outil permettant de saboter le système comme le spécifie le 8.7.2.1 dans l'EUT sans provoquer de détérioration physique avant que le dispositif de détection de la fraude ne fonctionne.

NOTE L'outil peut être introduit dans toute ouverture, avant ou pendant l'ouverture du boîtier. Pour les grades 3 et 4, cela inclut les ouvertures réservées aux voyants et aux organes de commande accessibles à un utilisateur de niveau 1.

Si l'outil est inséré avec succès, il convient qu'il soit manipulé afin de tenter d'interférer avec le dispositif de détection de la fraude. L'essai réalisé sur le fil vérifie la bonne formation des fils le cas échéant.

Les tentatives doivent être limitées à 5 min par outil (10 min pour le grade 4). Si l'essai échoue, il convient que celui-ci soit répété et un autre échec au cours de 4 autres tentatives doit se traduire par l'échec final de l'essai.

e) Mesure

Enregistrer la génération du signal ou du message d'auto surveillance.

f) Critères de réussite/d'échec

L'ouverture normale du CIE/de l'ACE ne doit être possible qu'en suivant la procédure définie par le fabricant et doit déclencher un signal ou un message d'auto surveillance.

a) soit le fonctionnement du dispositif de détection de la fraude ne doit pas être entravé avant la génération d'un signal ou d'un message d'auto surveillance,

b) soit une détérioration visible a été provoquée afin d'entraver le fonctionnement du dispositif de détection de la fraude.

11.8.4 Détection de la fraude – Enlèvement du support

a) Principe

Le principe de cet essai consiste à enlever le CIE/l'ACE de sa surface de montage et à surveiller l'EUT afin de déterminer si un signal ou un message d'auto surveillance est généré au cours de la période de temps requise lorsque la distance maximale autorisée (voir le 8.7.2.2) est dépassée.

b) Conditions d'essai

Il convient que le CIE se trouve dans l'état hors service.

c) Montage

Positionner l'EUT sur une surface plane horizontale en tenant compte des exigences spécifiées par le fabricant pour procéder à l'enlèvement depuis le dispositif de détection de montage.

d) Procédure

Soulever l'EUT depuis la surface plane dans une direction perpendiculaire à la surface de montage d'une distance supérieure à celle spécifiée dans le 8.7.2.2 tout en surveillant la sortie du signal ou du message d'auto surveillance.

Tenter de glisser une lame d'essai tel que défini dans le 8.7.2.2 pour faire échec à l'enlèvement depuis le dispositif de détection de montage avant et pendant l'essai ci-dessus.

Tenter de faire usage de pinces comme spécifié dans le 8.7.2.2 pour faire échec à l'enlèvement depuis le dispositif de détection de montage avant et pendant l'essai ci-dessus.

Les tentatives doivent être limitées à 5 min par outil (10 min pour le grade 4). Si l'essai échoue, il convient que celui-ci soit répété et un autre échec au cours de 4 autres tentatives doit se traduire par l'échec final de l'essai.

e) Mesure

Surveiller la sortie du signal ou du message d'auto surveillance.

Enregistrer s'il a été possible d'empêcher la génération d'un signal ou d'un message d'auto surveillance en utilisant la lame ou les pinces d'essai.

f) Critères de réussite/d'échec

Le signal ou le message d'auto surveillance doit avoir été généré dans les 11 s après le moment où l'EUT dépasse la distance spécifiée dans le 8.7.2.2.

Il doit être impossible d'empêcher la génération d'un signal ou d'un message d'auto surveillance en utilisant la lame ou les pinces d'essai.

11.8.5 Détection de la fraude – Pénétration dans le boîtier

a) Principe

Le principe de cet essai consiste à percer un trou dans une face accessible du boîtier et à vérifier qu'un signal ou un message d'auto surveillance est généré (voir le 8.7.2.3).

b) Conditions d'essai

Il convient que le système I&HAS se trouve dans l'état hors service.

c) Montage

Monter l'appareil en essai conformément aux instructions du fabricant avec le boîtier solidement fermé.

d) Procédure

Percer un trou de 4 mm de diamètre dans n'importe quelle face accessible de l'EUT à l'aide d'un foret en métal.

e) Mesure

Surveiller la sortie du signal ou du message d'auto surveillance.

f) Critères de réussite/d'échec

Un signal ou un message d'auto surveillance doit être généré lorsqu'un trou de 4 mm est percé dans une face accessible du boîtier.

11.9 Essais de substitution

11.9.1 Essais de surveillance de la substitution d'éléments

Le fabricant doit fournir des informations grâce auxquelles il est possible de vérifier que la méthode de surveillance est conforme à l'exigence de la CEI 62642-1, 8.7.3.

11.9.2 Essais de surveillance de la substitution – Exigences temporelles

Le fabricant doit fournir des informations grâce auxquelles il est possible de vérifier que la méthode de surveillance est conforme à l'exigence temporelle de la CEI 62642-1, 8.7.4.

11.10 Essais des performances temporelles de l'I&HAS

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme au 8.9 et à l'exigence temporelle de la CEI 62642-1, 8.8.1.

b) Principe

L'essai consiste à introduire un événement à déclarer puis à s'assurer qu'il a lieu dans le délai spécifié par la CEI 62642-1, 8.8.1 et 8.9.1.

c) Procédure

Avec le système en mode mise en service, déclencher un événement d'alarme relative à une intrusion.

d) Mesure

Enregistrer l'heure avant l'activation de la ou des sorties de notification.

e) Critères de réussite/d'échec

Le délai entre le déclenchement de l'événement et la notification ne doit pas dépasser 20 s.

Concernant les systèmes structurés de message:

- le fabricant doit fournir des informations permettant de déterminer l'heure à laquelle le message a été généré;
- le fabricant doit prouver que cette exigence temporelle peut être maintenue dans un système installé dans les conditions de communication les plus lentes possibles.

11.11 Essais d'interconnexions

11.11.1 Surveillance des interconnexions

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme au 8.8 et à l'exigence temporelle de la CEI 62642-1, 8.8.3.

b) Principe

L'essai consiste à simuler l'interconnexion désactivée et à surveiller la réponse.

NOTE Il peut s'avérer nécessaire pour le fabricant de fournir des informations détaillées relatives à la méthode à utiliser pour ce faire.

c) Procédure

a) Désactiver l'interconnexion (par exemple: par court-circuit).

b) Si le système utilise des interconnexions non spécifiques, simuler une autre application en contrôlant l'interconnexion en permanence.

d) Mesure

Enregistrer la réponse du système et mesurer le temps nécessaire au système pour répondre.

e) Critères de réussite/d'échec

Dans chacun des cas, la réponse doit être conforme aux exigences de la CEI 62642-1, 8.8.3.

11.11.2 Essais de surveillance de la communication périodique

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme au 8.8 et à l'exigence temporelle de la CEI 62642-1, 8.8.4.1.

b) Principe

Le fabricant doit fournir les moyens permettant:

a) de vérifier grâce à la documentation que la réponse du système est conforme aux exigences de la CEI 62642-1, Tableau 17,

ou

b) d'identifier le moment où a lieu une communication périodique afin de soumettre à l'essai comme suit.

c) Procédure

Avec le système en mode mise en service, appliquer une condition de défaut (par exemple: court-circuit) à l'interconnexion, immédiatement après la période de communication identifiée.

d) Mesure

Mesurer le temps nécessaire au système pour répondre.

e) Critères de réussite/d'échec

La réponse du système définie par la CEI 62642-1, Tableau 20, doit avoir lieu dans le délai spécifié par la CEI 62642-1, Tableau 17.

11.11.3 Essais de vérification au cours de la procédure de mise en service

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à être conforme au 8.8 et à l'exigence temporelle de la CEI 62642-1, 8.8.4.2.

b) Principe

Le fabricant doit fournir les moyens permettant:

a) de vérifier grâce à la documentation que la réponse du système est conforme aux exigences de la CEI 62642-1, Tableau 18,

ou

b) d'identifier le moment où a lieu une communication périodique afin de soumettre à l'essai comme suit.

c) Procédure

Avec le système en mode mise hors service, appliquer une condition de défaut (par exemple: court-circuit) à l'interconnexion, immédiatement après la période de communication identifiée pour la période requise par le Tableau 18. Tenter de mettre l'I&HAS en service.

d) Mesure

Surveiller l'état de l'I&HAS.

e) Critères de réussite/d'échec

L'I&HAS ne doit pas se mettre en service.

11.11.4 Essai relatif à la sécurité de la communication

Le fabricant doit fournir des informations permettant de vérifier la conformité aux exigences de la CEI 62642-1, 8.8.5.

11.12 Journal d'événements

a) Objet de l'essai

L'essai a pour objet de démontrer la capacité du CIE à tenir un journal d'événements et à conserver une horloge précise conformément aux exigences du 8.10.

b) Principe

L'essai consiste à activer le CIE afin de garantir le bon fonctionnement du journal d'événements, tout en assurant la précision à long terme de l'horloge (voir le Tableau 31).

c) Condition d'essai

L'essai doit être réalisé avec le système initialement dans l'état hors service.

Tableau 31 – Essai du journal d'événements

	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
1	Avec le CIE hors service et sans condition d'alarme, régler l'heure et la date.	Noter la date et l'heure.	
2	Avec le système hors service et à l'état normal, saisir un code à chaque niveau d'accès.	Noter les fonctions accessibles pour chaque niveau d'accès.	Aucune fonction ne doit permettre à l'utilisateur de modifier ou de supprimer le journal d'événements.
3	Si le moyen d'enregistrement est cyclique: Renseigner le journal d'événements. Avec le système hors service, ajouter un événement obligatoire supplémentaire	Noter les 2 événements les plus anciens avant l'ajout de l'événement final. Noter l'événement le plus ancien après l'ajout de l'événement final.	L'événement le plus ancien doit être supprimé par les événements obligatoires récemment ajoutés.

	Procédure d'essai (d)	Mesure (e)	Critères de réussite/d'échec (f)
4	Si le CIE dispose d'une fonction d'enregistrement des événements non obligatoires, saisir alors le nombre adapté d'événements obligatoires tel que défini dans la CEI 62642-1, 8.10. Renseigner le reste du journal d'événements avec des événements non obligatoires. Ajouter un événement non obligatoire.	Noter les événements obligatoires enregistrés dans le journal d'événements.	Vérifier que le nombre minimal autorisé d'événements obligatoires a été respecté.
5	Suite à l'essai précédent (C), ajouter un événement obligatoire.	Noter les événements obligatoires enregistrés dans le journal d'événements.	Vérifier que le nouvel événement obligatoire a été enregistré.
6	Si le ou les composants de mémorisation sont non volatiles (par exemple, EEPROM): Contrôler les données fournies par le fabricant.		Vérifier que les composants de stockage sont non volatiles pendant la période requise par la CEI 62642-1, Tableau 21.
7	Si les composants de mémorisation sont volatiles (par exemple RAM): Retirer l'EPS et l'APS du système pendant la période requise par la CEI 62642-1, Tableau 21. À l'issue de cette période, appliquer à nouveau la tension et contrôler le journal d'événements.	Enregistrer le contenu du journal d'événements avant d'éteindre et après avoir rallumé l'alimentation.	Le contenu du journal d'événements ne doit pas être perdu ou corrompu, à l'exception de l'ajout d'événements provoqués par cette procédure d'essai (par exemple: coupure secteur)
8	Dans le cas d'un CIE disposant d'une fonction d'enregistrement permanent, suivre les instructions du fabricant afin de procéder à un enregistrement permanent.	Noter le journal d'événements et les événements enregistrés dans l'enregistrement permanent.	Les événements affichés dans l'enregistrement permanent doivent refléter le journal d'événements avec précision, y compris la date et l'heure.
9	Contrôler la précision de l'horloge.	Lorsque le système fonctionne depuis une période d'au moins 8 jours, noter l'heure indiquée par le CIE.	La précision doit être conforme à la CEI 62642-1, 8.10.
Lorsque l'I&HAS stocke des journaux d'événements au niveau de l'ARC, le fabricant doit fournir des informations ou des moyens permettant de soumettre cette fonction à l'essai comme suit:			
10	Contrôler la capacité du CIE à envoyer des événements au SPT. Générer un événement au niveau du CIE.	Surveiller la sortie au SPT.	Vérifier que les événements générés sont envoyés au SPT.
11	Contrôler la capacité du CIE à indiquer le défaut de transmission à l'ARC. Désactiver le SPT et générer un nombre d'événements obligatoires conformément à la CEI 62642-1, 8.10, à reporter au niveau de l'ARC.	Enregistrer l'indication et la notification au niveau du CIE.	Vérifier qu'un défaut est indiqué au niveau du CIE (grade 1).
12	Activer le SPT.		Pour les CIE de grades 2, 3 et 4, les événements doivent être transmis lorsque le SPT est réactivé.

11.13 Marquage et documentation

a) Principe

Le principe de cet essai consiste à vérifier que le marquage du CIE et que la documentation fournie avec le CIE répondent aux exigences des Articles 9 et 10.

b) Procédure

Examiner le marquage du CIE et de l'ACE.

Examiner la documentation fournie par le fabricant CIE.

c) Critères de réussite/d'échec

Le marquage apposé sur le CIE et l'ACE doit répondre aux exigences de l'Article 10 de la présente norme.

La documentation doit satisfaire aux exigences de l'Article 9 de la présente norme.

NOTE Des essais de durabilité relatifs au marquage sont effectués dans le cadre des essais de la directive relative aux basses tensions.

11.14 Essais d'environnement et essais de compatibilité électromagnétique (CEM)

La classification environnementale est décrite dans la CEI 62642-1. Les essais d'environnement applicables effectués doivent être conformes à la CEI 62599-1.

Si l'essai fonctionnel réduit est spécifié durant le conditionnement environnemental et CEM, il doit être effectué conformément aux détails donnés dans la CEI 62599-1.

Pour les essais de fonctionnement, le CIE et l'ACE ne doivent pas générer de signal ou de message d'alarme, d'auto surveillance, de défaut ou autre ou passer d'un mode à un autre, lorsqu'ils sont soumis à une gamme spécifiée de conditions environnementales et CEM et doivent continuer à fonctionner normalement.

Pour les essais d'endurance, le CIE et l'ACE doivent réussir l'essai fonctionnel réduit après avoir été soumis à la gamme spécifiée de conditions environnementales.

Voir le Tableau 32 relatif aux essais applicables pour chaque classe d'environnement. Ces essais s'appliquent à tous les grades de sécurité.

Tableau 32 – Essais d'environnement et essais de compatibilité électromagnétique (CEM)

	Essai fonctionnel réduit (11.3)	Essai	Type	Classe I	Classe II	Classe III	Classe IV
1	B, D, A	Chaleur sèche	Opérationnel	M	M	M	M
2	B, A	Chaleur sèche	Endurance	N/A	N/A	N/A	M
3	B, D, A	Froid	Opérationnel	M	M	M	M
4	B, D, A	Chaleur humide, état stable	Opérationnel	M	N/A	N/A	N/A
5	B, A	Chaleur humide, état stable	Endurance	M	M	M	M
6	B, D, A	Variation de température (p)	Opérationnel	M	M	M	M
7	B, D, A	Chaleur humide, cyclique	Opérationnel	N/A	M	M	M
8	B, A	Chaleur humide, cyclique	Endurance	N/A	N/A	M	M
9	B, C, A	Infiltration d'eau	Opérationnel	M (p)	M (p)	M	M
10	B, A	Dioxyde de soufre (SO_2)	Endurance	N/A	N/A	M	M
11	B, A	Brouillard salin, cyclique	Endurance	N/A	N/A	N/A	M
12	B, C, A	De choc (f) (m)	Opérationnel	M	M	M	M
13	B, C, A	Chute libre (m) (p)	Opérationnel	M	M	M	M
14	B, C, A	Choc (f)	Opérationnel	M	M	M	M
15	B, C, A	Vibrations (sinusoïdales)	Opérationnel	M	M	M	M
16	B, C, A	Essais CEM	Opérationnel	M	M	M	M

Légende

A Après le conditionnement et la période de récupération.

B Avant le conditionnement.

C Surveiller pendant le conditionnement avec le CIE en mode mise en service.

D Pendant le conditionnement, surveiller avec le CIE en mode mise en service et procéder à l'essai fonctionnel réduit tel que spécifié dans la CEI 62599-1.

M Obligatoire.

N/A Non applicable.

(f) Applicable à l'équipement fixe.

(m) Applicable à l'équipement déplaçable.

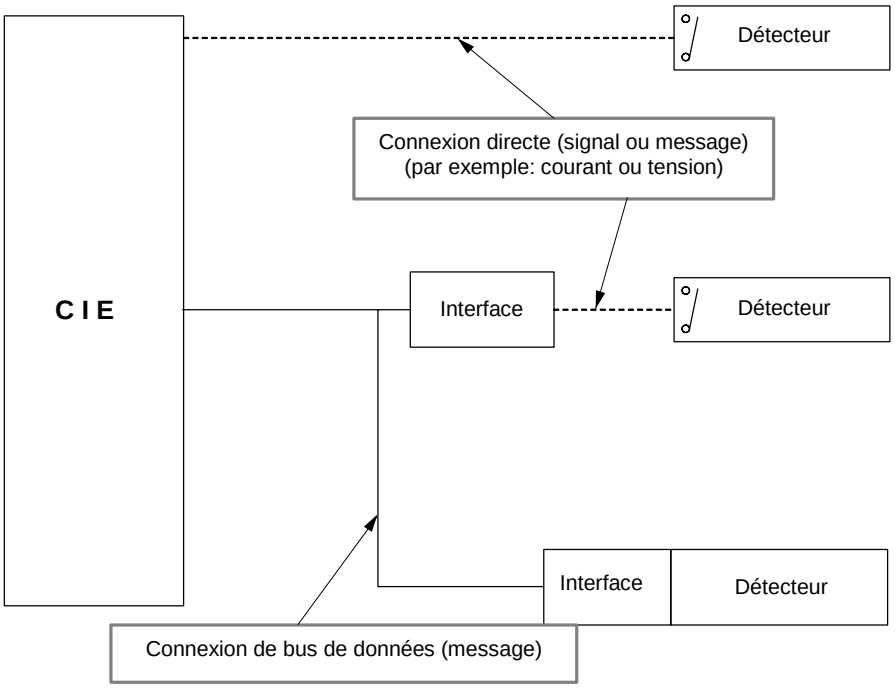
(p) Applicable à l'équipement portatif.

Annexe A
(informative)

Types d'interconnexion

La présente annexe vise à clarifier les termes définis dans la CEI 62642-1, Article 3.

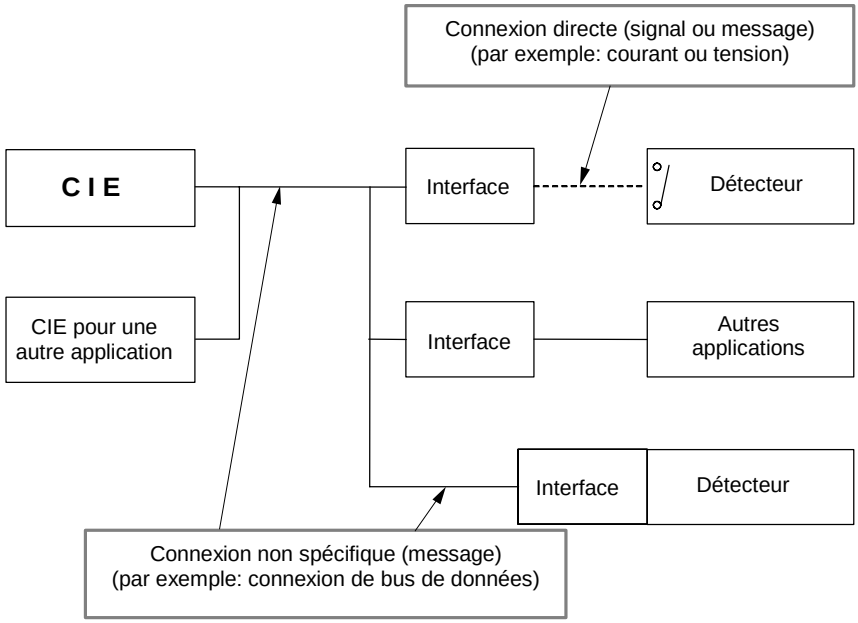
A.1 Interconnexions câblées spécifiques



NOTE Les interfaces peuvent prendre plusieurs formes (par exemple: extension, dispositif capable d'accepter des entrées d'un certain nombre de détecteurs, module destiné à jouer le rôle d'interface d'un détecteur unique, etc.).

Figure A.1 – Interconnexions câblées spécifiques

A.2 Interconnexions câblées non spécifiques



NOTE Les interfaces peuvent prendre plusieurs formes (par exemple: extension, dispositif capable d'accepter des entrées d'un certain nombre de détecteurs, module destiné à jouer le rôle d'interface d'un détecteur unique, etc.).

Figure A.2 – Interconnexions câblées non spécifiques

A.3 Interconnexions sans fil

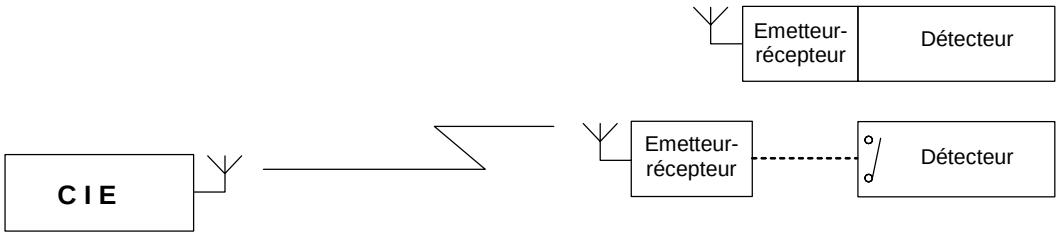


Figure A.3 – Interconnexions sans fil

Les interconnexions sans fil doivent être conformes aux exigences de la CEI 62642-5-3.

A.4 Signaux – Période active

Lorsqu'une connexion directe est utilisée entre le CIE et le détecteur et que les informations sur l'alarme sont envoyées comme un signal électrique, la période active du signal est alors la période pendant laquelle le relais de sortie du détecteur (ou le contact magnétique, ou encore le courant ou la tension électrique) se trouve en condition d'alarme.

Annexe B
(informative)

Résumé des exigences temporelles

Tableau B.1 – Tableau des caractéristiques temporelles

	Référence	Traiter si plus de	Traiter et notifier dans un délai de	Minimum	Maximum
Signal d'intrusion	8.9	400 ms	10 s		
Signal d'alarme contre les hold-up	8.9	400 ms	10 s		
Signal d'auto surveillance	8.9	400 ms	10 s		
Signal de défaut	8.9	10 s	10 s		
Signal de masquage – traité comme une intrusion	8.9 / CEI 62642-1, 8.4.5	400 ms	10 s		
Signal de masquage – traité comme un défaut	8.9 / CEI 62642-1, 8.4.5	10 s	10 s		
Signal de réduction importante de la plage de détection – traité comme une intrusion	8.9 / CEI 62642-1, 8.4.6	400 ms	10 s		
Réduction importante de la plage de détection – traité comme un défaut	8.9 / CEI 62642-1, 8.4.6	10 s	10 s		
Retard d'activation WD après notification à distance	8.6			0	10 min
Durée WD	8.6			90 s	15 min
Défaut EPS	8.6	10 s	1 h [a]		
Principal programme Watchdog	8.4.3	10 s	30 s [a]		
Durée de "l'indication de mise en service" après MISE EN SERVICE	8.3.3				[b]
Durée de "l'indication de mise hors service" après MISE HORS SERVICE	8.3.4				30 s
Durée de la procédure de mise hors service	8.3.4				45 s

[a] Peut être annulé si la condition est corrigée au cours de cette période.

[b] Cette indication est spécifiée comme "temps limité" - mais aucune limite réelle n'est spécifiée dans la CEI 62642-1. La limitation de durée ne s'applique pas aux systèmes de grade 1 et 2 utilisant la CEI 62642-1, 8.3.7, option c).

Annexe C
(normative)

Utilisation d'une interface non-I&HAS

Un niveau de contrôle de l'I&HAS peut être répété par un dispositif ne faisant pas partie de l'I&HAS (par exemple: un ordinateur ou un PDA). Le CIE peut fournir une passerelle logique destinée à la connexion d'un tel dispositif, qui peut être connecté par tout moyen adapté, qui peut être fixe ou portatif et qui peut se trouver à l'intérieur ou à distance des locaux surveillés.

Les protocoles de logiciel de communication doivent veiller à ce que la substitution, la sécurité des messages et l'intégrité des autorisations soient conformes aux exigences du Tableau C.1.

Le dispositif de commande peut être configuré pour fonctionner avec plusieurs I&HAS ou un ou plusieurs autre(s) systèmes.

Toutes les actions du système initiées par l'interface non-I&HAS doivent être identifiées de façon univoque dans le journal d'événements du CIE.

En raison de la nature des connexions et des protocoles utilisés, certaines exigences relatives au système I&HAS sont inadaptées (par exemple les protocoles de logiciel sécurisé pour remplacer la nécessité d'une protection contre la fraude); par conséquent, les conditions modifiées suivantes doivent s'appliquer à l'interface et aux connexions non-I&HAS:

Tableau C.1 – Conditions d'utilisation d'une interface non-I&HAS à des fins de commande et d'indication

CEI 62642-3	Fonction	Comportement attendu
7	Exigences environnementales	Non applicable
8.3.2	Autorisation	L'accès au logiciel de communication au niveau de l'interface non-I&HAS doit être conforme à la présente exigence.
	Authentification	Le démarrage de la communication entre l'interface non-I&HAS et l'I&HAS doit avoir une authentification équivalente aux exigences du 8.3.2.
8.5.1	Indications	Les indications à l'interface non-I&HAS peuvent être considérées comme équivalentes à un tableau synoptique (voir en 8.5.1, NOTE 3).
8.7.1	Protection contre la fraude	Non applicable
8.7.2	Détection de la fraude	Non applicable
8.7.3	Surveillance de la substitution	L'exigence doit s'appliquer à tous les grades. [a]
8.7.3	Exigences temporelles	L'exigence relative au grade 3 doit s'appliquer également aux grades 1 et 2. [a]
8.8	Surveillance des interconnexions	L'exigence de la CEI 62642-1, 8.8.3 (Tableau 16) ne s'applique pas aux dispositifs portatifs.
8.8	Sécurité de la communication	L'exigence de la CEI 62642-1, 8.8.5 (Tableau 19) doit s'appliquer à tous les grades.
8.11	Alimentation	L'exigence de la CEI 62642-1, 9.2 relative à l'APS n'est pas applicable.
[a] Si le dispositif ne peut pas assurer d'entrée à l'I&HAS, cette exigence n'est pas applicable.		

Annexe D
(informative)

Résumé des références croisées relatives à la fonction

Tableau D.1 – Références croisées

CEI 62642-1	CEI 62642-3	Fonction	Grade					Essai(s)
			1	2	3	4		
8.1	-	Détection						-
	8.1	Entrées						-
8.1.1	8.1.1	Détection d'intrusion	M	M	M	M		11.4.1
8.1.2	8.1.2	Déclenchement du dispositif du système d'alarme contre les hold-up	Op	Op	Op	Op		11.4.2
8.1.3	8.1.3	Détection de la fraude	M	M	M	M		11.4.3
8.1.4 (T.1)	8.1.4	Identification des pannes	M	M	M	M		11.4.4
	8.1.5	Utilisateur	M	M	M	M		11.5.1
8.2.1	8.1.6	Masquage	Op	Op	M	M		11.4.5
8.2.2	8.1.7	Réduction de la plage de détection du détecteur	Op	Op	Op	M		11.4.6
	8.1.8	Autres entrées	Op	Op	Op	Op		11.4.7
	8.2	Sorties	Op	Op	Op	Op		
8.3	8.1.5 / 8.3 / 8.4.2	Fonctionnement (commandes)	M	M	M	M		11.5.1
8.3.1 (T.2)	8.3.1	Niveaux d'accès	M	M	M	M		11.5.1
8.3.2 (T.3)	8.3.2	Autorisation	M	M	M	M		-
	8.3.2.1	Clés mécaniques	Op	Op	Op	Op	Doit inclure au moins un élément de la liste	11.6.1
	8.3.2.2	Clés logiques	Op	Op	Op	Op		11.6.2
	8.3.2.2.1	Codes PIN	Op	Op	Op	Op		11.6.2.2
	8.3.2.2.2	Clés numériques	Op	Op	Op	Op		11.6.2.1
	8.3.2.2.3	Clés biométriques	Op	Op	Op	Op		11.6.2.3
	8.3.2.3	Combinaisons de clés	Op	Op	Op	Op		11.6.2.4
	8.3.2.4	Répétition de codes invalides	Op	M	M	M		11.6.3
8.3.3	8.3.3 / 8.3.4	Mise en service/mise hors service	M	M	M	M		11.7.1 – 11.7.5
8.3.4	8.3.3	Mise en service	M	M	M	M		11.7.1, 11.7.5
8.3.5 (T.4)	8.3.3.1	Interdiction de mise en service	M	M	M	M		11.7.2
8.3.6 (T.5)	8.3.3.1	Annulation de l'interdiction de mise en service	Op	Op	Op	Op		11.7.2; 11.7.5
	8.3.3.2	Fonction de dernière issue	Op	Op	Op	Op		11.7.1
	8.3.3.3	Echec de mise en service	M	M	M	M		11.7.1
8.3.7	8.3.3.4	Etat de mise en service	M	M	M	M		11.7.3
8.3.8.1	8.3.4	Mise hors service	M	M	M	M		11.7.4; 11.7.5
8.3.8.2	8.3.4	Mise hors service selon 8.3.7 b de la CEI 62642-1(avec fonction de première issue)	Op	Op	Op	Op		11.7.4
8.3.9 (T.6)	8.3.5	Restauration	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1

CEI 62642-1	CEI 62642-3	Fonction	Grade					Essai(s)
			1	2	3	4		
8.3.10	8.3.6	Inhibition	Op	Op	Op	Op		11.5.1; 11.7.1; 11.7.6
-	8.3.6.1	Inhibition automatique	Op	Op	Op	Op		-
8.3.11	8.3.7	Isolation	Op	Op	Op	Op		11.5.1; 11.7.6
8.3.12	8.3.8	Essai utilisateur niveau 2	M	M	M	M		11.7.7
-	8.3.9	Essai d'immersion	Op	Op	Op	Op		11.7.7
8.3.13	8.3.10	Autres fonctions	Op	Op	Op	Op		11.7.8
8.4 (T.7)	8.4	Traitement	M	M	M	M		11.4.1
8.4.1	8.4.1 8.4.1.1	Signaux/messages d'intrusion	M	M	M	M		11.4.1
8.4.2	8.4.1	Signaux/messages d'alarme contre les hold-up	Op	Op	Op	Op		11.4.2
8.4.3	8.4.1	Signaux/messages d'auto surveillance	M	M	M	M		11.4.3
8.4.4	8.4.1	Signaux/messages de défaut	M	M	M	M		11.4.4
8.4.5	8.4.1	Signaux/messages de masquage	Op	Op	M	M		11.4.5
8.4.6	8.4.1	Signaux/messages de réduction de la plage de détection	Op	Op	Op	M		11.4.6
	8.4.1.2	Priorités	M	M	M	M		11.4.1
	8.4.2	Entrée utilisateur	M	M	M	M		11.5.1
	8.4.3	Surveillance du traitement du CIE	Op	Op	M	M		11.7.9
8.5.1 (T.8)	8.5.1	Indications - généralités	M	M	M	M		11.4.1/2/3/4/5/6
8.5.2 (T.9)	8.5.1 et 8.5.1.1	Disponibilité des indications	M	M	M	M		11.4.1/2/3/4/5/6 11.7.10
	8.5.1.2	Autres indications	Op	Op	Op	Op		11.4.7
8.5.3	8.5.1	Annulation des indications	M	M	M	M		11.4.1/2/3/4/5/6 11.7.10
	8.5.2	Indications visuelles	M	M	M	M		-
	8.5.3	Priorités	M	M	M	M		-
8.5.4	-	Indication – Systèmes d'alarme contre l'intrusion	-	-	-	-		-
8.6 (T.10 et T.11)	8.6	Notification	M	M	M	M		11.4.1/2/3/4/5/6
8.7.1	8.7.1	Protection contre la fraude	M	M	M	M		11.8.2
8.7.2 (T.12 et T.13)	8.7.2	Détection de la fraude						
	8.7.2.1	Ouverture du boîtier	M	M	M	M		11.8.3
	8.7.2.2	Enlèvement du support	Op	Op	M	M		11.8.4
	8.7.2.3	Pénétration dans le boîtier	Op	Op	Op	M		11.8.5
8.7.3 (T.14)	8.7.3	Surveillance de la substitution	Op	Op	Op	M		11.9
8.7.4 (T.15)	8.7.3	Substitution - minutage	Op	Op	Op	M		11.9
8.8.1	8.8	Interconnexions – généralités	M	M	M	M		11.10
8.8.2	8.8	Interconnexions – disponibilité	M	M	M	M		11.11
8.8.3 (T.16)	8.8	Interconnexions – surveillance	M	M	M	M		11.11

CEI 62642-1	CEI 62642-3	Fonction	Grade					Essai(s)
			1	2	3	4		
8.8.4.1 (T.17)	8.8	Vérification – communication périodique	M	M	M	M		11.11
8.8.4.2 (T.18)	8.8	Vérification – au cours de la période de mise en service	M	M	M	M		11.11
8.8.5 (T.19)	8.8	Sécurité de la communication	Op	Op	Op	M		11.11
8.8.6 (T.20)	8.8	Signaux/messages générés (Paragraphes 8.8.3 / 8.8.4 / 8.8.5) de la CEI 62642-1	M	M	M	M		11.11
8.9.1	8.9	Minutage – intrusions, fraude, défauts	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
8.9.2	8.9	Traitement	M	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
8.10 (T.21 et T.22)	8.10	Enregistrement d'événements	Op	M	M	M		11.4.1/2/3/4/5/6; 11.5.1;
	8.10.1	Enregistrement d'événements au niveau du CIE	Op	M	M	M		11.12
	8.10.2	Enregistrement d'événements au niveau de l'ARC	Op	Op	Op	Op		11.12
9.1	-	Types de PS	-	-	-	-		-
9.2 (T.24)	-	Exigences relatives au PS	-	-	-	-		-
	8.11	Alimentation	M	M	M	M		EN 50131-6
10	-	Fiabilité opérationnelle	M	M	M	M		-
11	-	Fiabilité fonctionnelle	M	M	M	M		-
12	7	Exigences environnementales	M	M	M	M		11.14
12.2	-	Compatibilité électromagnétique	M	M	M	M		11.14 et EMCD
13	-	Sécurité électrique	M	M	M	M		LVD
14.1	-	Documentation I&HAS						
14.2	9	Documentation relative au produit	M	M	M	M		11.13
15	10	Marquage/identification	M	M	M	M		11.13
M = Obligatoire Op = Facultatif								
NOTE Il convient de soumettre à essai toutes les fonctions I&HAS fournies et revendiquées par le fabricant (voir en 4.1).								

Bibliographie

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

CEI 62642-2 (toutes les parties), *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 2: Détecteurs d'intrusion*

EN 50136 (toutes les parties), *Systèmes d'alarme – Systèmes et équipements de transmission d'alarme*

CLC/TS 50398, *Systèmes d'alarme – Systèmes d'alarme combinés et intégrés – Règles générales*

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