

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

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

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviations	10
3.1 Terms and definitions	10
3.2 Abbreviations	13
4 Equipment attributes	13
4.1 General.....	13
4.2 Functionality.....	14
5 CIE construction.....	14
6 Security grade	14
7 Environmental performance	14
7.1 Requirements.....	14
7.2 Environmental and EMC tests	15
8 Functional requirements	15
8.1 Inputs.....	15
8.1.1 Intruder detection	15
8.1.2 Hold-up device	15
8.1.3 Tamper.....	15
8.1.4 Fault.....	15
8.1.5 User input.....	16
8.1.6 Masking.....	16
8.1.7 Movement detector range reduction.....	16
8.1.8 Non-I&HAS inputs	16
8.2 Outputs	16
8.3 Operation	16
8.3.1 Access levels	17
8.3.2 Authorization	17
8.3.3 Setting procedures	19
8.3.4 Unsetting procedure	20
8.3.5 Restore function	20
8.3.6 Inhibit function.....	20
8.3.7 Isolate operation.....	21
8.3.8 Verification of I&HAS functions	21
8.3.9 Alarm point soak test mode	21
8.3.10 Other functions	21
8.4 Processing	21
8.4.1 Processing of input signals or messages	21
8.4.2 Processing of user inputs	22
8.4.3 Monitoring of CIE processing.....	22
8.5 Indication	23
8.5.1 General	23
8.5.2 Visual indicators	24
8.5.3 Priority of indications	24
8.6 Notification outputs.....	24

8.6.1	Other notification	24
8.7	Tamper security (detection/protection)	24
8.7.1	Tamper protection	25
8.7.2	Tamper detection.....	25
8.7.3	Monitoring of substitution.....	27
8.8	Interconnections.....	27
8.9	Timing.....	27
8.10	Event recording.....	27
8.10.1	Event recording at the CIE.....	28
8.10.2	Event recording at the ARC or other remote location	28
8.11	Power supply.....	28
9	Product documentation.....	29
9.1	Installation and maintenance	29
9.2	Operating instructions	30
10	Marking and labelling	30
11	Tests	30
11.1	Test conditions	30
11.1.1	Laboratory conditions and tolerance	30
11.1.2	Mounting	30
11.1.3	CIE test configuration	31
11.1.4	Power supply.....	31
11.1.5	Event log checks	31
11.1.6	Documentation	32
11.2	Test procedures	32
11.2.1	Tolerances	32
11.2.2	Wire-free devices	32
11.3	Reduced functional test.....	32
11.4	Functional tests.....	33
11.4.1	Processing intruder alarm signals or messages	33
11.4.2	Processing of hold-up signals or messages	35
11.4.3	Processing of tamper signals or messages	37
11.4.4	Processing of fault signals or messages	38
11.4.5	Processing masking signals or messages	40
11.4.6	Processing reduction of range signals or messages.....	42
11.4.7	CIE processing in the presence of non-I&HAS inputs.....	43
11.5	Access level.....	44
11.5.1	Access to the functions and controls.....	44
11.6	Authorization requirements.....	45
11.6.1	Mechanical key tests	45
11.6.2	Logical key tests.....	46
11.6.3	Invalid authorization attempts	48
11.7	Operational tests.....	49
11.7.1	Setting procedures	49
11.7.2	Prevention of setting and overriding of prevention of setting procedures	51
11.7.3	The set state	52
11.7.4	Unsetting procedures	52
11.7.5	Setting and/or unsetting automatically at pre-determined times	54
11.7.6	Inhibit and isolate functions.....	55

11.7.7	Test functions.....	57
11.7.8	Other functions.....	57
11.7.9	Monitoring of CIE processing.....	58
11.7.10	Availability of indications.....	59
11.8	Tamper security tests.....	59
11.8.1	ACE type A.....	59
11.8.2	Tamper protection.....	59
11.8.3	Tamper detection – Access to the inside of the housing.....	60
11.8.4	Tamper detection – Removal from mounting.....	61
11.8.5	Tamper detection – Penetration of the housing.....	62
11.9	Substitution tests.....	62
11.9.1	Tests for monitoring of substitution of components.....	62
11.9.2	Tests for monitoring of substitution – Timing requirements.....	62
11.10	Testing of I&HAS timing performance.....	62
11.11	Testing for interconnections.....	63
11.11.1	Monitoring of interconnections.....	63
11.11.2	Testing of monitoring of periodic communication.....	63
11.11.3	Testing of verification during setting procedure.....	64
11.11.4	Test for security of communication.....	65
11.12	Event log.....	65
11.13	Marking and documentation.....	66
11.14	Environmental and EMC tests.....	66
Annex A (informative)	Interconnection types.....	68
Annex B (informative)	Summary of timing requirements.....	70
Annex C (normative)	Use of non-I&HAS interface.....	71
Annex D (informative)	Summary of function cross-references.....	72
Bibliography		75
Figure A.1	– Specific wired interconnections.....	68
Figure A.2	– Non-specific wired interconnections.....	69
Figure A.3	– Wire-free interconnections.....	69
Table 1	– Recognition of additional fault conditions.....	15
Table 2	– Recognition of biometric keys.....	18
Table 3	– Time intervals for methods of authorization used in combination.....	18
Table 4	– Detection of repeated invalid authorization attempts.....	19
Table 5	– Monitoring of processing.....	22
Table 6	– Indications supplementary to those of IEC 62642-1.....	23
Table 7	– Tamper protection.....	25
Table 8	– Tamper detection.....	26
Table 9	– Tool dimension for tamper detection.....	26
Table 10	– Removal from mounting.....	26
Table 11	– Additional events to be included in event log.....	27
Table 12	– Reduced functional test.....	33
Table 13	– Tests of the processing of intruder signals or messages.....	34
Table 14	– Tests of the processing of hold-up signals or messages.....	36

Table 15 – Tests of the processing of tamper signal or messages.....	37
Table 16 – Test of processing of fault signals or messages.....	39
Table 17 – Test of processing of masking signals or messages	41
Table 18 – Test of processing of reduction of range signals or messages	42
Table 19 – Test of CIE processing in the presence of non-I&HAS inputs.....	44
Table 20 – Test of the access to the functions and controls	44
Table 21 – Test for disabling user input device by invalid keys	48
Table 22 – Test for generation of tamper signal or message by invalid keys	49
Table 23 – Test of setting procedure.....	50
Table 24 – Test of prevention of setting and overriding of prevention of setting procedure	51
Table 25 – Test for unsetting procedure.....	53
Table 26 – Test of setting and/or unsetting automatically at pre-determined times	55
Table 27 – Inhibit and isolate functions	56
Table 28 – Verification of test functions	57
Table 29 – Test of CIE process monitoring.....	58
Table 30 – Test of availability of indications.....	59
Table 31 – Test of event log	65
Table 32 – Environmental and EMC tests	67
Table B.1 – Timing table	70
Table C.1 – Conditions for use of non-I&HAS interface for control and indicating purposes.....	71
Table D.1 – Cross-references	72

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 to the 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 regional directive.

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, 8.3.10) 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.