IEC 62642-1

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems – Intrusion and hold-up systems – Part 1: System requirements

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

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

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62642-1

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems – Intrusion and hold-up systems – Part 1: System requirements

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 13.320

ISBN 978-2-88910-970-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM SYSTEMS – INTRUSION AND HOLD-UP SYSTEMS –

Part 1: System requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62642-1 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

This standard is based on EN 50131-1 (2006) and its Amendment 1 (2009).

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

FDIS	Report on voting
79/280/FDIS	79/299/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 result 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 standard is part of the IEC 62642 series of International Standards and Technical Specifications "*Alarm systems – Intrusion and hold-up systems*", written to include the following parts:

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	Requirements for interconnections equipment using radio frequency techniques
Part 6	Power supplies
Part 7	Application guidelines
Part 8	Security fog devices

This International Standard applies to Intrusion and Hold-up Alarm Systems (I&HAS). The standard is also intended to apply to Intruder Alarm Systems (IAS) which include only intrusion detectors and to Hold-up Alarm Systems (HAS) which include only hold-up devices.

This International Standard is a specification for Intrusion and Hold-up Alarm Systems installed in buildings, it includes four security grades and four environmental classes.

The purpose of an I&HAS is to enhance the security of the supervised premises. To maximise its effectiveness an I&HAS should be integrated with appropriate physical security devices and procedures. This is particularly important to higher grade I&HAS.

This standard is intended to assist insurers, intruder alarm companies, customers and the police in achieving a complete and accurate specification of the supervision required in particular premises, but it does not specify the type of technology, the extent or degree of detection, nor does it necessarily cover all of the requirements for a particular installation.

All references to the requirements for I&HAS refer to basic minimum requirements and the designers of such installed I&HAS should take into account the nature of the premises, the value of the contents, the degree of risk of intrusion, the threat to personnel and any other factors which may influence the choice of grade and content of an I&HAS.

Recommendations for design, planning, operation, installation and maintenance are given in Application Guidelines EN/TS 50131-7.

This standard is not intended to be used for testing individual I&HAS components. Requirements for testing individual I&HAS components are given in the relevant component standards.

I&HAS and components thereof are graded to provide the level of security required. The security grades take into account the risk level which depends on the type of premises, the value of the contents, and the typical intruder or robber expected.

ALARM SYSTEMS – INTRUSION AND HOLD-UP SYSTEMS –

Part 1: System requirements

1 Scope

This part of IEC 62642 specifies the requirements for Intrusion and Hold-up Alarm Systems (I&HAS) installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to the components of an I&HAS installed in a building which are normally mounted on the external structure of a building e.g. ancillary control equipment or warning devices. The standard does not include requirements for exterior I&HAS.

This International Standard specifies performance requirements for installed I&HAS but does not include requirements for design, planning, installation, operation or maintenance.

These requirements also apply to I&HAS sharing means of detection, triggering, interconnection, control, communication and power supplies with other applications. The functioning of an I&HAS is not adversely influenced by other applications.

Requirements are specified for I&HAS components where the relevant environment is classified. This classification describes the environment in which an I&HAS component may be expected to function as designed. 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 Annex A. General environmental requirements for I&HAS components are described in Clause 7.

The requirements of this standard also apply to IAS and HAS when these systems are installed independently.

When an I&HAS does not include functions relating to the detection of intruders, the requirements relating to intrusion detection do not apply.

When an I&HAS does not include functions relating to hold-up, the requirements relating to hold-up do not apply.

NOTE Unless otherwise stated, the abbreviation I&HAS is also intended to mean IAS and HAS.

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 60065:2001, *Audio, video and similar electronic apparatus – Safety requirements*

IEC 60950-1:2005, *Information technology equipment – Safety – Part 1: General requirements*

IEC 61000-6-3:2006, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments*

IEC 62599-1:2010, *Alarm systems – Part 1: Environmental test methods*

IEC 62599-2:2010, *Alarm systems – Part 2: Electromagnetic compatibility – Immunity requirements for components of fire and security alarm systems*

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

EN 50136-1-1:1998, *Alarm systems – Alarm transmission systems and equipment – Part 1-1: General requirements for alarm transmission systems*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
action
(relating to setting and unsetting) deliberate operation or act by the user which is part of the setting or unsetting procedure

3.1.2
access level
level of access to particular functions of an I&HAS

3.1.3
active
state of a detector in the presence of a hazard

3.1.4
active period
period during which an alarm signal is present

3.1.5
alarm
warning of the presence of a hazard to life, property or the environment

3.1.6
alarm receiving centre
continuously manned centre to which information concerning the status of one or more I&HAS is reported

3.1.7
alarm company
organization which provides services for I&HAS

3.1.8
alarm condition
condition of an I&HAS, or part thereof, which results from the response of the system to the presence of a hazard

3.1.9
alarm notification
passing of an alarm condition to warning devices and/or alarm transmission systems

---

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

3.1.10
alarm system
electrical installation which responds to the manual or automatic detection of the presence of a hazard

3.1.11
alarm transmission system
equipment and network used to transfer information from one or more I&HAS to one or more alarm receiving centres

NOTE Alarm transmission systems exclude local direct connections, i.e. interconnections between parts of an I&HAS which do not require an interface to transform the I&HAS information into a form suitable for transmission.

3.1.12
alert indication
audible and/or visual indication, available at access level 1, when an I&HAS is in the unset state, indicating that further indication(s) are available to users at access levels 2, 3, or 4

3.1.13
alternative power source
power source capable of powering the I&HAS for a predetermined time when a prime power source is unavailable

3.1.14
ancillary control equipment
equipment used for supplementary control purposes

3.1.15
application
electronic security system

EXAMPLE Social alarm, CCTV, access control or fire system or a non-security electronic/electrical system such as heating, air conditioning, lighting, etc.

3.1.16
authorisation
permission to gain access to the various control functions of an I&HAS

3.1.17
authorisation codes
mechanical or logical keys which permit access to I&HAS functions

3.1.18
availability of interconnection
condition when an interconnection is capable of conveying a signal or message

3.1.19
component substitution
the replacement of I&HAS components with alternative devices which prevent an I&HAS functioning as designed

3.1.20
communication
transmission of messages and/or signals between I&HAS components

NOTE The transmission of a signal may include the continual passing of an electrical current through a switch or relay forming the interface between I&HAS components. It is not necessary to change the status of any such switch or relay. Due to the nature of data communication, the transmission of a message may require deliberate initiation,

e.g. in response to a poll or at specified time intervals, this initiation may or may not require the change of status of a switch or relay.

3.1.21
continually
recurring frequently at regular intervals

3.1.22
control and indicating equipment
equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information

3.1.23
entry/exit route
route by which authorized entry or exit to the supervised premises or part thereof may be achieved

3.1.24
event
condition arising from the operation of an I&HAS e.g. setting/unsetting or the functioning of an I&HAS, e.g. alarm signal or message

3.1.25
event recording
storage of events arising from the operation e.g. setting or unsetting of an I&HAS or the functioning of an I&HAS for future analysis

3.1.26
fault condition
condition of an alarm system which prevents an I&HAS or parts thereof from functioning normally

3.1.27
fault signal
fault message
information generated due to the presence of a fault

3.1.28
hold-up alarm system
alarm system providing the means for a user to deliberately generate a hold-up alarm condition

3.1.29
hold-up device
device which when triggered causes a hold-up alarm signal or message to be generated

3.1.30
hold-up alarm condition
condition of an alarm system, or part thereof, which results from the response of an I&HAS to the triggering of a hold-up device

3.1.31
indication
information (in audible, visual or any other form) provided to assist the user in the operation of an I&HAS

3.1.32
inhibit
status of a part of an I&HAS in which an alarm condition cannot be notified, such status remaining until the I&HAS or part thereof passes from the set to the unset status

3.1.33
interconnection
means by which messages and/or signals are communicated between I&HAS components

3.1.34
interconnection media
medium by which signals or messages are conveyed

3.1.35
interference
corruption of signals and/or messages passing between I&HAS components

3.1.36
intruder alarm system
alarm system to detect and indicate the presence, entry or attempted entry of an intruder into supervised premises

3.1.37
intruder alarm condition
condition of an I&HAS, or part thereof, which results from the response of the I&HAS to the presence of an intruder

3.1.38
intruder signal
intruder message
information generated by an intruder detector

3.1.39
intrusion detector
device designed to generate an intruder signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard

3.1.40
intrusion and hold-up alarm system
combined intruder and hold-up alarm system

3.1.41
isolation
status of a part of an alarm system in which an alarm condition cannot be notified, such status remaining until cancelled by a user

3.1.42
masked
condition whereby the field of view of a movement detector is blocked

3.1.43
message
series of signals routed via interconnections which include identification, function data and the various means for providing its own integrity, immunity and proper reception

3.1.44
message substitution
intentional or unintentional creation of alternative message between I&HAS components which prevent the correct functioning of an I&HAS

3.1.45
monitoring
process of verifying that interconnections and equipment are functioning correctly

3.1.46
non-specific wired interconnection
interconnection conveying information pertaining to two or more applications

3.1.47
normal condition
state of an I&HAS where no conditions exist which would prevent the setting of an I&HAS

3.1.48
notification
passing of an alarm, tamper or fault condition to warning devices and/or alarm transmission systems

3.1.49
operator
authorised individual (a user) using an I&HAS for its intended purpose

3.1.50
override
intervention, by a user, to permit setting when an I&HAS is not in a normal condition

3.1.51
part set
status of an I&HAS in which an intruder or hold-up alarm condition can be notified but part of the I&HAS is unset

3.1.52
pending indication
means of indicating that further information is available for display when all information cannot be displayed simultaneously

3.1.53
periodic communication
any valid signal or message

3.1.54
power supply
part of an alarm system which provides power for an I&HAS or any part thereof

3.1.55
prime power source
power source used to support an I&HAS under normal working conditions

3.1.56
restore
procedure of canceling an alarm, tamper, fault or other condition and returning an I&HAS to a previous condition

3.1.57
self powered device
device incorporating its own power sources

3.1.58
sensor
part of a detector which senses a change in condition

3.1.59
set
status of an I&HAS or part thereof in which an intruder or hold-up alarm condition can be notified

3.1.60
signal
variable parameters by which information is conveyed

3.1.61
significant reduction of range
reduction of the detection range of a movement detector, measured on the central axis of the detector, exceeding 50 % of specified range

3.1.62
site specific data
information relating to the configuration of an I&HAS e.g. processing parameters

3.1.63
specific wired interconnection
interconnection conveying information pertaining to one application

3.1.64
standby period
period during which the alternative power source is capable of supporting an I&HAS

3.1.65
subsystem
part of an I&HAS located in a clearly defined area of the supervised premises capable of functioning independently of other parts of the I&HAS

3.1.66
supervised premises
part of a building and/or area in which an intrusion, attempted intrusion, or the triggering of a hold-up device may be detected by an I&HAS

3.1.67
supplementary prime power source
energy source (independent of the prime power source) capable of supporting an I&HAS for extended periods, without affecting the standby period of the alternate power source

3.1.68
system components
individual items of equipment which constitute an I&HAS when configured together

3.1.69
supervised premises transceiver
equipment at the supervised premises, including the interface to the I&HAS and the interface to the alarm transmission network

3.1.70
tamper
deliberate interference with an I&HAS or part thereof

3.1.71
tamper alarm
alarm generated by tamper detection

3.1.72
tamper condition
condition of an I&HAS in which tampering has been detected

3.1.73
tamper detection
detection of deliberate interference with an I&HAS or part thereof

3.1.74
tamper protection
methods or means used to protect an I&HAS or part thereof against deliberate interference

3.1.75
tamper security
methods or means used to protect an I&HAS or part thereof against deliberate interference and the detection of deliberate interference with an I&HAS or part thereof

3.1.76
tamper signal
tamper message
information generated by a tamper detector

3.1.77
transmission path
a transmission path between an individual alarm system and its associated alarm receiving centre(s)

3.1.78
triggering
deliberate operation of a hold-up device

3.1.79
unset
status of an I&HAS or part thereof in which an intruder and/or hold-up alarm condition cannot be notified

3.1.80
user
person authorised to operate an I&HAS

3.1.81
user interface
means by which a user operates an I&HAS

3.1.82
warning device
a device that gives an audible alarm in response to a notification

NOTE 1 A warning device may also provide alert indications.

NOTE 2 Such indications should be easily distinguishable from those related to the notification of an alarm condition.

3.1.83
wire-free interconnection
interconnection conveying information between I&HAS components without physical media

3.1.84
zone
area of the supervised premises where an intrusion, attempted intrusion, or the triggering of a hold-up device may be detected by an I&HAS

NOTE Although a zone could contain just one detector, the term “zone” is not synonymous with one detector input. A zone may include any number of detectors. Examples of zones include: a storey of a building, the perimeter of a building, an outbuilding.

3.2 Abbreviations

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

ARC – alarm receiving centre
ACE – ancillary control equipment
ATS – alarm transmission system
CIE – control and indicating equipment
HAS – hold-up alarm system(s)
IAS – intruder alarm system(s)
I&HAS – intrusion and hold-up alarm system(s)
WD – warning device
PS – power supply
SPT – supervised premises transceiver

4 System functions

I&HAS shall include, as appropriate to the configuration of the I&HAS, the functions specified in this standard for the detection of intruders and/or triggering, processing of information, notification of alarms and the means to operate an I&HAS.

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.

5 System components

I&HAS components shall be classified according to their environmental capability and graded according to their performance.

I&HAS components shall be compatible within an I&HAS and selected according to the system grade and appropriate environmental classification.

Components of other applications may be combined or integrated with an I&HAS, providing the performance of the I&HAS components is not adversely influenced.

6 Security grading

I&HAS shall be given a security grading which will determine its performance. The grading shall be one of four grades with grade 1 being the lowest grade and grade 4 the highest. The grade of an I&HAS shall be that of the lowest graded component.

When an I&HAS is divided into clearly defined sub-systems, an I&HAS may include components of differing grades within each sub-system. The grade of a subsystem shall be that of the lowest graded component within it.

Components shared by more than one sub-system shall have a grade equal to that of the highest sub-system grade (e.g. control and indicating equipment/alarm transmission systems/warning devices/power supplies).

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

NOTE 1 For the guidance of specifiers and those responsible for the security of premises, the following grades are given:

Grade 1: Low risk

An intruder or robber is expected to have little knowledge of I&HAS and be restricted to a limited range of easily available tools.

Grade 2: Low to medium risk

An intruder or robber is expected to have a limited knowledge of I&HAS and the use of a general range of tools and portable instruments (e.g. a multi-meter).

Grade 3: Medium to high risk

An intruder or robber is expected to be conversant with I&HAS and have a comprehensive range of tools and portable electronic equipment.

Grade 4: High risk

To be used when security takes precedence over all other factors. An intruder or robber is expected to have the ability or resource to plan an intrusion or robbery in detail and have a full range of equipment including means of substitution of components in an I&HAS.

NOTE 2 In the all grades, the term “Intruder” is intended to embrace other types of threat (e.g. robbery or the threat of physical violence, which might influence the design of an I&HAS).

7 Environmental classification

7.1 General

Components shall be suitable for use in one of the following environmental classes. Environmental test requirements for I&HAS components are given in the individual component standards. IEC 62599-1 describes the environmental test methods to be applied to I&HAS components.

NOTE 1 Classes I, II, III and IV are progressively more severe and therefore Class IV components may, for example, be used in Class III I&HAS.

I&HAS components shall operate correctly when exposed to environmental influences specified in 7.2, 7.3, 7.4 and 7.5. For each class, typical information is given below.

NOTE 2 Annex A includes special national conditions for specified countries.

NOTE 3 The environmental conditions described in Clause 7 are those in which an I&HAS is expected to perform correctly, they are not necessarily the conditions to be used during the testing of I&HAS components.

7.2 Environmental Class I – Indoor

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

NOTE Temperatures may be expected to vary between +5 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.3 Environmental Class II – Indoor – General

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

NOTE Temperatures may be expected to vary between –10 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.4 Environmental Class III – Outdoor – Sheltered or indoor extreme conditions

Environmental influences normally experienced out of doors when I&HAS components are not fully exposed to the weather or indoors where environmental conditions are extreme.

NOTE Temperatures may be expected to vary between –25 °C and +50 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year, relative humidity can be expected to vary between 85 % and 95 % non-condensing.

7.5 Environmental Class IV – Outdoor – General

Environmental influences normally experienced out of doors when I&HAS components are fully exposed to the weather.

NOTE Temperatures may be expected to vary between –25 °C and +60 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year, relative humidity can be expected to vary between 85 % and 95 % non-condensing.

8 Functional requirements

8.1 Detection of intruders, triggering, tampering and the recognition of faults

I&HAS shall include, as appropriate to its configuration, means for the detection of intruders, triggering, tampering and the recognition of faults necessary to meet the requirements of this standard.

NOTE When an I&HAS is configured as an IAS, i.e. only including intrusion detectors, it is not necessary for the system to provide the functionality required of a HAS. Similarly when an I&HAS is configured as an HAS, it is not necessary for the system to provide functionality required of an IAS.

Other events may be detected providing this does not adversely influence the mandatory requirements for the detection of intruders, triggering, tampering and the recognition of faults.

8.1.1 Intruder detection

Detectors shall be suitable for the environment and application and may incorporate more than one technology.

Detectors shall be designed and installed so as to maximise the detection of genuine intrusion and minimise the risk of false alarms

An intruder signal or message shall be generated for the required duration when an intrusion detector has been activated. This duration shall be as necessary to ensure communication is achieved.

8.1.2 Hold-up device – triggering

I&HAS shall, as appropriate, include hold-up devices which are suitable for the environment and application.

Hold-up devices shall include means to minimise the possibility of accidental triggering.

A hold-up signal or message shall be generated when a hold-up device has been in an active condition for the required duration. This duration shall be as necessary to ensure communication is achieved.

8.1.3 Tamper detection

Tamper detection shall be incorporated in all I&HAS components as specified in Table 12.

A tamper signal or message shall be generated for the required duration when a tamper detector has been activated. This duration shall be as necessary to ensure communication is achieved.

8.1.4 Recognition of faults

Dependent upon the grade of an I&HAS, means shall be provided to recognise the fault conditions specified in Table 1.

A fault signal or message shall be generated for the required duration when a fault has been present for the required period. This duration shall be as necessary to ensure communication is achieved.

Table 1 – Faults

Faults	Grade 1	Grade 2	Grade 3	Grade 4
Detector(s)	M	M	M	M
Hold-up device(s)	M	M	M	M
Prime power source	M	M	M	M
Alternative power source	M	M	M	M
Interconnections	M	M	M	M
Alarm transmission system(s) [a]	M	M	M	M
Warning device(s)	M	M	M	M
Other faults [b]	Op	Op	Op	Op

Key: M = Mandatory Op = Optional.

NOTE The requirement for I&HAS to recognise detector, hold-up device, ATS and WD faults does not imply such equipment is required to provide a dedicated faults output, for example a WD fault may be derived from a failure of periodic communication.

[a] Where an I&HAS is required by its grade and notification option to have more than one alarm transmission system, a fault on any ATS is recognised.

[b] Other faults as specified in components standards.

8.2 Other functions

8.2.1 Masking

In grade 3 and 4, I&HAS movement detectors shall include means to detect masking.

8.2.2 Movement detector range reduction

In grade 4, I&HAS movement detectors shall include the means to detect significant reduction of specified range.

8.3 Operation

I&HAS shall be designed to minimise the possibility of an operator generating a false alarm.

Controls, e.g. keypad buttons, used during the operation of an I&HAS shall be clearly and unambiguously marked and logically arranged in such a manner as to minimise the possibility of incorrect operation.

8.3.1 Access levels

This standard specifies four levels of user access that categorise the ability of users to access the system components and controls.

The four access levels are as follows.

Level 1 Access by any person

Functions required to be accessible at level 1 shall have no restriction on access.

Level 2 User access e.g. by an operator

Functions affecting the operational status (without changing an I&HAS configuration, e.g. site specific data).

Access to functions required to be accessible at level 2 shall be restricted by means of a key or code operated switch or lock or other equivalent means. Level 2 key or codes shall not provide access at level 3 or level 4.

Level 3 User access e.g. by alarm company personnel

All functions affecting an I&HAS configuration (without changing equipment design).

Access to functions required to be accessible at level 3 shall be restricted by means of a key or code operated switch or lock or other equivalent means. Level 3 key or codes shall not provide access at level 4.

Level 4 User access e.g. by the manufacturer of the equipment

Access to components to change equipment design.

Access to functions required to be accessible at level 4 shall be restricted by means of a key or code operated switch or lock or other equivalent means.

NOTE Access level 4 applies when changing the operating programme software without having activated a tamper device on the CIE or ACE.

Access at level 3 shall be prevented unless either

a) access has been permitted by a user with level 2 access, or
b) in grades 1, 2 and 3 I&HAS, access at level 3 may be provided without authorisation by a level 2 user providing
   1) the user to be given access at level 3 is at the supervised premises and accesses the CIE locally, and
   2) the I&HAS is unset, and

3) in grade 1, I&HAS notification is given by a warning device when the access at level 3 is granted,

4) in grades 2 and 3, notification is given by a warning device and remotely, i.e. by an ATS, when the access at level 3 is granted.

Access at level 4 shall be prevented until access has been authorized by a user with level 2 access and by a user with level 3 access.

Access at levels 2, 3 and 4 may be achieved remotely providing authorisation, equivalent to that specified in Table 3, is achieved.

The functions accessible at each level are described in Table 2.

Table 2 – Levels of access

Functions	Access levels			
	1	2	3 [a]	4 [b]
Setting	NP [e]	P	P	NP
Unsetting	NP	P	P	NP
Restore I&HAS	NP	P	P	NP
Verify I&HAS functions	NP	P	P	NP
Interrogate event log	NP	P	P	NP
Inhibit/isolate/override [c]	NP	P	P	NP
Add/change individual authorisation codes	NP	P [d]	P [d]	P [d]
Add/delete level 2 users & codes	NP	P	P	NP
Add/change site specific data	NP	NP	P	NP
Change/replace basic programme	NP	NP	NP	P

Key: P = Permitted NP = Not permitted.

NOTE 1 The inclusion of the functions shown in this table does not imply that provision of such functions in I&HAS is mandatory.

NOTE 2 This table specifies access levels for each function; further conditions, applicable to each function, are specified elsewhere in this standard.

NOTE 3 Requirements relating to user access are not intended to restrict methods of initialisation of user access at the time that the CIE is first powered-up (e.g. the existence of default or single use access codes).

[a] Only when authorised at level 2.

[b] Only when authorised at level 2 and level 3.

[c] Depending on the grade.

[d] An individual is only permitted to change his/her own user code.

[e] Permitted only in grade 1, see 8.3.4.

8.3.2 Authorisation

Permission to gain access to functions of an I&HAS shall be restricted by the use of authorisation codes or equivalent means as specified in Table 3.

Table 3 – Authorisation code requirements

Access levels 2, 3, and 4	Grade 1 differs	Grade 2 differs	Grade 3 differs	Grade 4 differs
Logical key	1 000	10 000	100 000	1 000 000
Mechanical key	300	3 000	15 000	50 000
NOTE Reference to mechanical and logical keys in the above table does not exclude the use of other means of authorisation, e.g. biometrics.				

8.3.3 Setting and unsetting

There shall be facilities to restrict access to the means of setting and unsetting to user(s) with the appropriate level of access.

Means shall be provided to enable a user with the appropriate level of access, to set and unset an I&HAS whilst minimising the possibility of incorrect operation.

It is permitted to provide means to set and unset an IAS and an HAS and/or to set and unset parts of an IAS, HAS or I&HAS independently.

8.3.4 Setting

Setting of an I&HAS or part thereof shall be achieved by an authorised action provided all functions of the system, or part thereof, are in a normal condition. During the setting procedure, a setting indication may be provided.

Access levels 2 or 3 users are permitted to set all grades of I&HAS using authorisation codes or equivalent means as specified in Table 3, grade 1.

In grade 1 I&HAS users at access level 1 may start setting (e.g. by a pushbutton) provided that this setting process may also be cancelled before completion by a user at access level 1 and means to start setting is located inside the supervised premises.

NOTE Starting of setting of the system by users at access level 1 should be used with caution.

8.3.5 Prevention of setting

Setting of an I&HAS or part thereof shall be prevented, unless overridden as permitted in 8.3.6, when one or more of the conditions shown in Table 4 is present.

Table 4 – Prevention of setting

Prevention of setting conditions	Grade 1	Grade 2	Grade 3	Grade 4
Intrusion detector in active condition [a]	M	M	M	M
Hold up device in active condition	M	M	M	M
Movement detector masked	Op	Op	M	M
Movement detector range reduction	Op	Op	Op	M
Intrusion detector fault	Op	M	M	M
Tamper condition	Op	M	M	M
Interconnection faults	Op	M	M	M
Prime power source fault	Op	M	M	M
Alternative power source fault	Op	M	M	M
Alarm transmission system fault	Op	M	M	M
Warning device fault	Op	M	M	M

Prevention of setting conditions	Grade 1	Grade 2	Grade 3	Grade 4
ATS and WD faults [b]	M	M	M	M
Other faults	Op	M	M	M
Key: M = Mandatory Op = Optional.				
NOTE The inclusion of a condition in this table does not imply that the associated function is included in an I&HAS.				
[a] Intrusion detectors on an agreed exit route may be excluded.				
[b] Faults in all available ATS and WD's which prevent all notification.				

8.3.6 Overriding prevention of setting

Conditions preventing setting may be overridden by users with the access levels specified in Table 5. Overriding shall be limited to each set period.

Overriding of prevention of set conditions shall be recorded in the event log.

It shall not be possible to override a prevention of set condition if overriding would result in the generation of an alarm condition.

Table 5 – Overriding of prevention of setting conditions

Prevention of setting conditions	Grade 1	Grade 2	Grade 3	Grade 4
Intruder detector in active condition [a]	Access level 2	Access level 2	Access level 2	Access level 2
Hold up device in active condition	Access level 2	Access level 2	Access level 2	Access level 2
Movement detector masked	Access level 2	Access level 2	Access level 2	Access level 2
Movement detector range reduction	Access level 2	Access level 2	Access level 2	Access level 2
Intruder detector fault	Access level 2	Access level 2	Access level 2	Access level 2
Tamper condition	Access level 2	Access level 2	Access level 3	Access level 3
Interconnection faults	Access level 2	Access level 2	Access level 3	Access level 3
Prime power source fault	Access level 2	Access level 2	Access level 2	Access level 2
Alternative power source fault	Access level 2	Access level 2	Access level 2	Access level 3
Alarm transmission system fault	Access level 2	Access level 2	Access level 3	Access level 3
Warning device fault	Access level 2	Access level 2	Access level 3	Access level 3
ATS and WD faults [b]	Access level 2	Access level 2	Access level 3	Access level 3
Other faults	Access level 2	Access level 2	Access level 2	Access level 3
NOTE The inclusion of the conditions in this table does not imply that the associated functions is provided.				
[a] Intrusion detectors on an agreed exit route may be excluded.				
[b] Faults in all available ATS and WD's which prevent all notification.				

8.3.7 Set state

When the setting procedure has been satisfactorily completed there shall be a time limited completion of setting indication to show the system or part thereof has changed to a set state.

NOTE The completion of setting indication should be of sufficient duration to enable a user to ascertain the status of an I&HAS.

In grades 1 and 2 I&HAS when an I&HAS or part thereof is in a set state:

a) access to the supervised premises or part thereof, via an entry/exit route, shall be prevented, or

b) opening the door to the entry/exit route shall initiate an entry procedure, or

c) indication of the set/unset status shall be provided.

In grades 3 and 4 I&HAS when an I&HAS or part thereof is in a set state:

d) access to the supervised premises or part thereof, via an entry/exit route, shall be prevented, or

e) opening the door to the entry/exit route shall initiate an entry procedure.

8.3.8 Unsetting

8.3.8.1 Unsetting – General

In all grades, unsetting of an I&HAS or part thereof shall be achieved by an authorised action.

8.3.8.2 Unsetting (as specified in 8.3.7 b))

When an I&HAS or part thereof is unset in accordance with 8.3.7 b) a route from the entry point to the means of unsetting shall be defined. Provided the correct entry procedure has been initiated only detectors in the defined route shall be ignored to permit access to the unsetting device.

NOTE 1 Unsetting by entering a supervised area via an entry/exit route is one means of unsetting. Unsetting without entering a supervised area is also permitted i.e. unsetting from outside the supervised area.

A maximum period of 45 s shall be permitted to complete the unsetting procedure. During this period, there shall be an entry indication. If unsetting is not completed within the defined period, e.g. the expiry of the entry time, an alarm condition shall be notified. When the unsetting procedure has been satisfactorily completed in accordance with the present subclause, there shall be a completion of unsetting indication to show the system or part thereof has changed to the unset state. The completion of unsetting shall be indicated for a maximum of 30 s (see Table 9).

When an intruder alarm condition occurs during the unsetting procedure, the alarm condition shall be notified by a warning device or indicated. When remote notification is included in the intruder alarm system, the alarm condition shall not be remotely notified until the indicator or warning device has functioned for a minimum of 30 s and the entry timer has expired.

NOTE 2 When an IAS is in the unsetting procedure, the indication referred to in the above paragraph is not restricted by the requirements of Table 9.

8.3.9 Restoring

I&HAS shall include the means necessary to restore the I&HAS or part thereof following an intruder, hold-up, tamper or fault condition. Access to the means of restoring shall be restricted to users with access levels specified in Table 6.

It is permitted to restore any grade of IAS remotely providing the requirements specified in 8.3.1 and 8.3.2 are achieved and information is available to determine the cause of condition to be restored.

Table 6 – Restoring

	Grade 1	Grade 2	Grade 3	Grade 4
Intruder	Access levels 2 or 3	Access levels 2 or 3	Access levels 2 or 3	Access levels 2 or 3
Hold-up	Access levels 2 or 3	Access levels 2 or 3	Access levels 2 or 3	Access levels 2 or 3
Tamper	Access levels 2 or 3	Access levels 2 or 3	Access level 3	Access level 3
Fault [a]	Access levels 2 or 3	Access levels 2 or 3	Access level 3	Access level 3

	Grade 1	Grade 2	Grade 3	Grade 4
Prime power source fault	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
ATS fault	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Masking	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Significant reduction of range	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
[a] Except prime power and ATS faults.				

8.3.10 Inhibit

I&HAS may include the means necessary to inhibit the functioning of individual or groups of functions. Access to the means of inhibiting shall be restricted to users with access levels 2 or 3.

8.3.11 Isolate

I&HAS may include the means necessary to isolate individual or groups of functions. Access to the means of isolation shall be restricted to users with the following access levels:

- grades 1 and 2 access levels 2 or 3;
- grades 3 and 4 access level 3.

8.3.12 Test

I&HAS 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 are non destructive.

8.3.13 Other functions

I&HAS may include the means necessary to carry out other operations not specifically included in this standard.

Other operations which directly or indirectly adversely influence the functions of an I&HAS shall be carried out by a user with access level 3.

8.4 Processing

Processing of signals or messages shall depend on the status, type of signal or message and the configuration of an I&HAS.

Table 7 specifies requirements for the processing of hold-up, intruder, tamper and fault signals and/or messages.

Individual detectors may be logically grouped requiring the generation of one or more intruder signals or messages from one or more detectors to generate an intruder alarm condition.

An individual detector may be configured to require more than one activation to generate an intruder alarm signal or message.

8.4.1 Intruder signals or messages

Signals and/or messages from intrusion detectors shall be processed as specified in Table 7. Following notification of an alarm condition, an I&HAS may remain capable of notifying further alarm conditions provided the maximum duration of functioning of the external audible WD is restricted in accordance with national or local regulations.

NOTE Multiple intruder alarm, tamper or fault conditions notified to an alarm receiving centre should be processed at the ARC to avoid unwanted response.

8.4.2 Hold-up signals or messages

Signals and/or messages from hold-up devices shall be processed as specified in Table 7.

After notification of a hold-up alarm condition(s), further signals and/or messages from hold-up devices shall continue to be processed as indicated in Table 7.

Multiple signals and/or messages from the same hold-up device need not be processed as required by Table 7 if they occur within less then 180 s of the previous signal or message.

8.4.3 Tamper signals or messages

Depending on the grade of an I&HAS, tamper signals or messages shall be processed as specified in Table 7.

8.4.4 Fault signals or messages

Dependent upon the grade of an I&HAS, fault signals or messages shall be processed as specified in Table 7.

8.4.5 Masking signals or messages

Masking signals or messages shall be processed as intruder or fault signals or messages in accordance with Table 7.

8.4.6 Reduction of range signals or messages

Reduction of range signals or messages shall be processed as intruder or fault signals or messages in accordance with Table 7.

Table 7 – Processing of intruder, hold-up, tamper alarm and fault signals/messages

		Grade 1				Grade 2				Grade 3				Grade 4			
I&HAS status [a]	**Inputs / Outputs**	**Hold-Up Signal/ Message**	**Intruder Signal/ Message**	**Tamper Signal/ Message**	**Fault Signal/ Message**	**Hold-Up Signal/ Message**	**Intruder Signal/ Message**	**Tamper Signal/ Message**	**Fault Signal/ Message**	**Hold-Up signal/ Message**	**Intruder signal/ Message**	**Tamper Signal/ Message**	**Fault Signal/ Message**	**Hold-Up signal/ Message**	**Intruder signal/ Message**	**Tamper Signal/ Message**	**Fault Signal/ Message**
Set	Indications	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	External audible alarm	Op	M	M	NP	Op	M	M	NP	Op	M	Op	NP	Op	M	Op	NP
	Internal audible alarm	Op	M	M	Op	Op	M	M	Op	Op	M	Op	Op	Op	M	Op	Op
	ATS Message Type	Hold-up	Intruder	Intruder or tamper	Intruder or fault	Hold-up [b]	Intruder	Intruder or tamper	Fault	Hold-up [b]	Intruder	Tamper	Fault	Hold-up [b]	Intruder	Tamper	Fault
Unset	Indications	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	External audible alarm	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP
	Internal audible alarm	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP
	ATS Message Type	Op as Hold-up	NP	Op as Tamper	Op as Fault	Op as Hold-up	NP	Op as Tamper	Op as Fault	Hold-up	NP	Tamper	Fault	Hold-up	NP	Tamper	Fault

Key: M = Mandatory Op = Optional NP = Not permitted.

NOTE 1 The inclusion in this table of requirements relating to warning devices and alarm transmission systems does not imply that I&HAS shall include such devices or systems; however, if such devices or systems are included in an I&HAS they shall comply with the requirements of this table.

NOTE 2 Cells containing Op, M or NP represent outputs to indicators, warning devices and ATS, the functioning of which is dependent on requirements specified in subclauses relating to those functions.

NOTE 3 Notwithstanding the specification of an item being shown as mandatory, when a notification option is not provided (see Table 10) inclusion of an output is not required.

NOTE 4 Requirements for indication should be read in conjunction with 8.5 and the functioning of indications is conditional upon the requirements of 8.5

NOTE 5 External WD shall not be activated by the CIE in the unset state, but may self-activate due to the activation of the WD tamper detection or the failure of the interconnection to the CIE.

[a] Signals and/or messages shall be processed according to the status of the I&HAS, IAS or HAS or part thereof.

[b] Information relating to the zone of the hold-up alarm to be included in the information transmitted to an ARC.

8.5 Indications

8.5.1 General

The indications specified in Table 8 shall be provided. When a function is not included in an I&HAS, the requirements for indications associated with that function need not be provided.

NOTE 1 As an example of the above when an I&HAS does not include a hold-up function, requirements for indication relating to hold-up need not be provided.

NOTE 2 Indications may be suppressed in certain cases, e.g. to avoid an indication in the event of the activation of a hold-up device.

When it is not possible for the indications provided to simultaneously display all mandatory available information, i.e. mandatory information waiting to be displayed, an indication shall be provided to indicate further information is available e.g. an “information pending” indicator.

An alert indication shall be provided when an I&HAS is unset to indicate conditions awaiting indication to a user.

All mandatory indications required by this clause shall be located together in at least one CIE or ACE. Further indications may be provided at other locations.

Where an I&HAS is required by its grade and notification option to have more than one alarm transmission system, a detectable fault on any of the transmission systems should be indicated to the person setting the system.

NOTE 3 The requirements of IEC 60073 apply only to indicators. Warning devices need not comply with IEC 60073.

NOTE 4 IEC 60073 includes requirements relating to the use of coloured indicators and does not necessarily apply when colour is not used as a means of differentiating indications, e.g. the use of a monochrome liquid crystal display.

Table 8 – Indication

Indications	Grade 1	Grade 2	Grade 3	Grade 4
I&HAS set/Part set	M	M	M	M
I&HAS unset	M	M	M	M
Hold-up alarm condition	M	M	M	M
Hold-up zone identification	M	M	M	M
Intruder alarm condition	M	M	M	M
Intruder zone identification	M	M	M	M
Individual intrusion detector indication (see 8.5.4) [a]	Op	Op	M	M
Detector alarm condition indicator (see 8.5.4)	M	M	M	M
Inhibited	M	M	M	M
Isolated	M	M	M	M
Fault conditions (see Table 1)	M	M	M	M
Tamper condition	M	M	M	M
Masking (see 8.2.1)	Op	Op	M	M
Range reduction (see 8.2.2)[d]	Op	Op	Op	M
Pending indication(s)	M	M	M	M
Alert indication	M	M	M	M
Setting (see 8.3.4) [b]	Op	Op	Op	Op
Completion of setting (see 8.3.7) [b]	M	M	M	M
Entry indication (see 8.3.8.2) [b, c]	M	M	M	M
Completion of unsetting (see 8.3.8.2) [b, c]	M	M	M	M

Key: M = Mandatory Op = Optional NOTE When a function, e.g. hold-up, is not provided the associated indication is not required.
[a] Individual detector identification applies only to detectors with processing capabilities, see 8.5.4. [b] These indications are time limited. [c] These indications are mandatory only when the optional unsetting procedure described in 8.3.8.2 is used. [d] May be the same indication as masking.

8.5.2 Availability of indications

Indications shall be available to users at access level 1 as specified in Table 9. The other indications included in Table 8 shall be available only to users who have accessed an I&HAS at access levels 2, 3 or 4.

Table 9 – Indications available during set and unset status at access level 1

Indications	Grade 1		Grade 2		Grade 3		Grade 4	
	Set	Unset	Set	Unset	Set	Unset	Set	Unset
I&HAS set/Part set [see 8.3.7 grades 1 and 2 c)]	Op	NA	Op	NA	NP	NA	NP	NA
I&HAS unset [see 8.3.7 grades 1 and 2 c)]	NA	Op	NA	Op	NA	NP	NA	NP
Alert indication	NP	M [c]	NP	M [c]	NP	M [c]	NP	M [c]
Setting (see 8.3.4) [a]	NA	Op	NA	Op	NA	Op	NA	Op
Completion of setting (see 8.3.7) [a]	M	NA	M	NA	M	NA	M	NA
Entry indication (see 8.3.8.2) [a, b]	M	NA	M	NA	M	NA	M	NA
Completion of unsetting (see 8.3.8.2) [a, b]	NA	M	NA	M	NA	M	NA	M
Key: Op = Optional NP = Not permitted NA = Not applicable M = Mandatory. NOTE 1 In grades 3 and 4 I&HAS, it is not considered acceptable to indicate, at access level 1, the set/unset state of an I&HAS. NOTE 2 When a function is not provided, the associated indication is not required.								
[a] These indications are time limited. [b] These indications are mandatory only when the optional unsetting procedure described in 8.3.8.2 is used. [c] This indication is optional if the I&HAS is part set.								

8.5.3 Cancelling indications

Indications, except time limited indications, specified in Table 8 shall remain available until cancelled by a user.

NOTE An alert indication shall be shown when an I&HAS is unset, other indications shall be available at access levels 2 and 3 when an I&HAS is set or unset.

It shall not be possible to cancel an indication until the condition causing the indication is no longer present.

8.5.4 Indication – Intrusion detectors

Intrusion detectors which include processing capability shall include individual means of indication of alarm conditions as specified in Table 8.

Intrusion detectors without processing capabilities are permitted to share a common means of indication. Not more than 10 such detectors are permitted to share a common means of indication.

8.6 Notification

Hold-up, intruder alarm, tamper and fault conditions and other conditions shall be notified by ATS and/or audible WD in accordance with the requirements specified in Tables 10 and 11. I&HAS shall include means of notification complying with at least one of the grade dependent options specified in Table 10.

The duration of the operational period of a WD may be subject to variation depending on local or national requirements.

The operation of WD may be suppressed, e.g. to avoid the operation of the WD in the event of the activation of a hold-up device.

Dependent upon the grade of I&HAS, when an alarm transmission system is included in an I&HAS the alarm transmission system shall comply with the requirements of EN 50136-1-1 at the performance criteria requirements specified in Table 11.

When an I&HAS includes both ATS and WD, it is permitted to delay the operation of the WD for a period not exceeding 10 min. It is permitted to suppress the operation of the WD providing notification to an alarm receiving centre or other receiving facility via an alarm transmission system is confirmed by the alarm receiving centre or other receiving facility during the delay period.

When a fault is detected in the alarm transmission system transmission path, any such delay in the operation of a WD shall be automatically cancelled provided that the fault or faults are detected in all available transmission paths.

Audible WD shall operate for a minimum of 90 s unless a shorter period is demanded by local or national regulations. The maximum operating period shall be 15 min unless a shorter period is demanded by local or national regulations.

Notification of prime power supply faults may be delayed for a maximum of 1 h.

The means of notification may be supplemented by non-mandatory means provided such devices do not impair the correct functioning of the mandatory devices e.g. mains driven siren or a device to impair vision (fog generating device).

Table 10 – Notification requirements

Notification Equipment	Grade 1			Grade 2				Grade 3				Grade 4			
	Options			Options				Options				Options			
	A	B	C	A	B	C	D	A	B	C	D	A	B	C	D
Remotely powered audible WD	2	Op	Op	2	Op	Op	Op	2	Op	Op	Op	2	Op	Op	Op
Self-powered audible WD	Op	1	Op	Op	1	Op	Op	Op	1	Op	Op	Op	1	Op	Op
Main ATS	Op	Op	ATS 1	ATS 2	ATS 2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6
Additional ATS	Op	Op	Op	Op	Op	ATS 1	Op	Op	Op	ATS 3	Op	Op	Op	ATS 4	Op

Key: Op = Optional.

NOTE 1 Digits in cells specify the number of audible warning devices to be included by grade and option.

NOTE 2 ATS 1, ATS 2, etc refers to the performance criteria as specified in Table 11.

NOTE 3 Where 2 ATS are specified, it is recommended that the transmission paths are independent and use

differing technologies, typically land-line and wireless.

NOTE 4 An SPT may be part of more than one ATS.

NOTE 5 The main and additional ATS shall meet their defined performance criteria when working normally. It is not a requirement of this standard for the performance of the additional ATS to change due to the failure of the main ATS.

Table 11 specifies ATS performance criteria as included in Table 10 in accordance with the requirements of EN 50136-1-1.

NOTE 1 Annex B includes an extract of performance requirements specified in EN 50136-1-1.

NOTE 2 This standard refers to performance requirements specified in EN 50136-1-1 but does not include requirements relating to the classification of availability.

Table 11 – Alarm transmission system performance criteria

Performance criteria	Transmission time classification	Transmission time max. values	Reporting time classification	Substitution security	Information security
ATS 1	D1	M1	T2	S0	I0
ATS 2	D2	M2	T2	S0	I0
ATS 3	D2	M2	T2	S1	I1
ATS 4	D2	M2	T3	S1	I2
ATS 5	D3	M3	T4	S2	I3
ATS 6	D4	M4	T6	S2	I3

8.7 Tamper security

8.7.1 Tamper protection

I&HAS components shall provide means to prevent access to internal elements to minimise the risk of tampering. Requirements for tamper protection may vary dependent on the grade of an I&HAS and whether an I&HAS component is located within or outside of the supervised area.

I&HAS components located external to the supervised premises shall have appropriate means of tamper protection (e.g. ancillary control equipment, warning devices).

All terminals and means of mechanical and electronic adjustment shall be located within component housings.

Housings shall be sufficiently robust to prevent undetected access to internal elements without visible damage.

Means of access to internal elements of control and indicating equipment, ancillary control equipment, alarm transmission systems, and warning devices shall be robust and mechanically secured. Normal access shall require the use of an appropriate tool.

Means of access to the internal elements of detectors and hold-up devices shall be secured and normal access shall require the use of a tool.

Access to means provided to adjust the field of view of a detector shall be made inaccessible to unauthorised persons.

8.7.2 Tamper detection

I&HAS components specified in Table 12 shall include means to detect tampering. Table 13 specifies the types of tampering to be detected. Tamper detection shall operate in both set and unset state in all grades.

Ancillary control equipment designed for use outside of the supervised premises shall include means to prevent the substitution of the ancillary control equipment and/or signals or messages between the ancillary control equipment and the control and indicating equipment. This requirement need not apply when any such substitution cannot influence the correct operation of an I&HAS.

Table 12 – Tamper detection – Components to include

Components	Grade 1	Grade 2	Grade 3	Grade 4
CIE/ACE [a]/SPT/WD/PS	M	M	M	M
Hold-up devices [a]	Op	M	M	M
Intrusion detectors [b]	Op	M	M	M
Junction boxes [c]	Op	Op	M	M
Key: Op = Optional M = Mandatory.				
[a] Portable ACE and hold-up devices are not required to comply with the requirements of this table.				
[b] It is accepted that it may be impractical to provide tamper detection to magnetically or mechanically actuated switches. However in certain grades, it may be necessary to protect magnetically actuated devices against tampering with an external magnetic or electro-magnetic source.				
[c] In grade 3, when an I&HAS includes protection against the substitution of signals or messages, junction boxes need not be provided with tamper detection.				

Table 13 – Tamper detection – Means to be detected

Means	Grade 1	Grade 2	Grade 3	Grade 4
Opened by normal means	M	M	M	M
Removal from mounting – Wire-free I&HAS components	Op	M	M	M
Removal from mounting – Wired I&HAS components	Op	Op	M [c]	M
Penetration of audible WD	Op	Op	Op	M [a]
Penetration of CIE/ACE/SPT	Op	Op	Op	M [a]
Detector orientation adjustment	Op	Op	M [b]	M [b]
Key: Op = Optional M = Mandatory.				
[a] Applies to CIE, ACE, SPT or WD when located outside the supervised premises.				
[b] When orientation adjustment is possible.				
[c] This requirement is optional for junction boxes and opening contacts (magnetic).				

8.7.3 Monitoring of substitution

Depending on the grade of an I&HAS, monitoring shall be provided to detect the substitution of I&HAS components. Monitoring shall comply with the requirements of Table 14. When an I&HAS is in a set or unset condition and substitution is detected, a tamper signal or message shall be generated.

Table 14 – Monitoring of substitution

Monitoring requirements	Grade 1	Grade 2	Grade 3	Grade 4
Substitution of I&HAS components	Op	Op	Op	M
Key: Op = Optional M = Mandatory.				

8.7.4 Monitoring of substitution – Timing requirements

Substitution of I&HAS components shall be detected within the times specified in Table 15.

Table 15 – Monitoring of substitution – Timing

Monitoring requirements	Grade 1 s	Grade 2 s	Grade 3 s	Grade 4 s
Substitution of I&HAS components	Op	Op	100 [a]	10
Key: Op = Optional.				
[a] When detection of substitution is included in grade of I&HAS.				

8.8 Interconnections

8.8.1 General

Interconnections shall be suitable for the purpose and designed to provide a reliable means of communication between I&HAS components.

Interconnections shall be designed to minimise the possibility of signals or messages being delayed, modified, substituted or lost, requirements for which are specified in the following subclauses.

Communication shall be established between I&HAS components to verify that the communication, necessary for the correct functioning of I&HAS can be accomplished as and when required (e.g. when an alarm signal or message is generated).

Interconnections shall be monitored to

a) detect when availability fails to meet the requirements specified in 8.8.2 and 8.8.3 below,

b) detect the delay, modification, substitution or loss of a signal or message as required in 8.8.5 below.

When interconnections are functioning normally, a signal or message shall be conveyed from the source to the destination component within 10 s.

When the interconnection media can be influenced from outside the supervised premises, special measures shall be taken to ensure that signals or messages cannot be delayed, modified, substituted or lost as specified in Table 19.

8.8.2 Availability of interconnections

Interconnections shall be available to provide a reliable means of conveying signals or messages.

When interconnections are shared with other applications, the availability of the interconnection to an I&HAS shall be sufficient to meet the requirements of this standard.

8.8.3 Monitoring of interconnections

Table 16 specifies the maximum permitted period for an interconnection to be unavailable. When the maximum permitted period is exceeded, a tamper or fault signal or message shall be generated as specified in Table 20. The requirements specified in 8.8.3 do not apply to portable hold-up devices and portable ACE.

Table 16 – Maximum unavailability of interconnections

	Grade 1 **s**	**Grade 2** **s**	**Grade 3** **s**	**Grade 4** **s**
Maximum permitted duration of unavailability	100	100	100	10
NOTE The requirement above is intended to establish if communication is possible by monitoring the communication media to ascertain if it is available to convey a signal or message. Monitoring may take the form of listening for jamming when RF techniques are employed or when an I&HAS shares a BUS system with other applications checking that another application has not taken permanent control of the BUS.				

In grades 1 and 2 I&HAS, when the time period between periodic communications (see 8.8.4.1) exceeds 100 s, the interconnection media shall be monitored to establish its availability to convey signals or messages.

8.8.4 Verification

8.8.4.1 Interconnection integrity – Periodic communication

Interconnection integrity shall be continually verified at intervals not exceeding those specified in Table 17. In the event of communication not being verified as specified in Table 17, signals or messages shall be generated as follows:

a) when communication cannot be verified because of an identified fault condition, a fault signal or message shall be generated as shown in Table 20;

b) when communication cannot be verified but no identified reason exists, a tamper or fault signal or message shall be generated as shown in Table 20.

Table 17 – Verification intervals

	Grade 1 min	**Grade 2** min	**Grade 3** s	**Grade 4** s
Maximum permitted intervals between periodic communication signals or messages	240	120	100	10

8.8.4.2 Verification during the setting procedure

Setting of an I&HAS shall be prevented when the last verification signal or message from any system component exceeds the periods specified in Table 18.

Table 18 – Maximum time period from last signal or message

	Grade 1 min	**Grade 2** min	**Grade 3** s	**Grade 4** s
Maximum time from the receipt of the last signal or message	60	20	60	10

8.8.5 Security of communication

Grade 4 I&HAS shall include means to detect the delay, modification, substitution or loss of any signals or messages as specified in Table 19.

The maximum permitted time period to detect the delay, modification, substitution or loss of any signal or message shall not exceed those shown in Table 17 plus 10 s.

In the event of a delay, modification, substitution or loss of any signal or message being detected a fault or tamper signal or message shall be generated as shown in Table 20.

Table 19 – Security of signals and messages

	Grade 1	Grade 2	Grade 3	Grade 4
Delay, modification, substitution or loss of signals or messages	Op	Op	Op	M
Key: Op = Optional M = Mandatory.				

8.8.6 Signals or messages to be generated

Signals or messages, arising from the requirement of the subclauses included in Table 20, shall be generated as specified in Table 20.

Table 20 – Signals or messages to be generated

Requirements	Grade 1	Grade 2	Grade 3	Grade 4
	Signal or message	Signal or message	Signal or message	Signal or message
Monitoring of interconnections (8.8.3)	T or F	T or F	T	T
Periodic communication (8.8.4.1 a)	F	F	F	F
Periodic communication (8.8.4.1 b)	T or F	T or F	T	T
Security of communication (8.8.5)	T or F	T or F	T	T
Key: T = Tamper F = Fault. NOTE The generation of signals or messages is required only when mandatory in the applicable subclause.				

8.9 I&HAS timing performance

8.9.1 Intruder detection, tampering, triggering, and the recognition of faults – Timing requirements

Intruder, hold-up, and tamper signals with an active period exceeding 400 ms shall be processed. Fault signals present for more than 10 s shall be processed.

NOTE Hold-up, intruder, tamper and fault messages need to be present only for the period necessary to ensure communication is successful.

8.9.2 Processing

Intruder, hold up, tamper and fault signals and/or messages shall be notified within 10 s.

8.10 Event recording

Dependent upon the grade of an I&HAS, the events specified in Table 22 shall be recorded.

The means used to record the mandatory events shall be protected against the accidental or deliberate deletion or alteration of the contents.

The means of recording events shall have a capacity complying with the requirements of Table 21. When the capacity of the means of recording is finite and the event recorder reaches maximum capacity, further events may cause the oldest events to be erased.

Grades 2, 3 and 4 I&HAS shall record, in addition to the event, the time and date at which the event occurred. The timing shall be accurate to within ± 10 min per annum at a nominal 20 °C.

The means of recording events may be included in I&HAS components or at an alarm receiving centre. When event recording is provided at an ARC or another remote location, an indication shall be provided if the transmission of events to the remote location has been unsuccessful. Grade 2, 3, and 4 I&HAS shall include means to store events awaiting transmission. Remote means of recording shall comply with the requirements of Table 21.

NOTE When the recording of events is accomplished in an alarm receiving centre, the means of notification necessary should be provided in an I&HAS. The means of recording events at an alarm receiving centre should comply with the requirements of 8.10.

In grades 3 and 4, a facility to make a permanent record of the events recorded shall be provided. This facility need not include the means of producing the permanent record.

The number of events recorded from any single source shall be limited to at least three and a maximum of 10 during any set or unset period.

Table 21 – Event recording – Memory

Capacity and endurance	Grade 1	Grade 2	Grade 3	Grade 4
Memory capacity – Minimum number of events	Op	250 events	500 events	1 000 events
Minimum endurance of memory after I&HAS power failure	Op	30 days	30 days	30 days
Key: Op = Optional.				

Table 22 – Event recording – Events to be recorded

Events	Grade 1	Grade 2	Grade 3	Grade 4
User identity when setting/unsetting (when possible)	Op	Op	M	M
Set/Part set	Op	M	M	M
Unset	Op	M	M	M
Hold-up alarm condition	Op	M	M	M
Hold-up zone identification	Op	Op	M	M
Intruder alarm condition	Op	M	M	M
Intruder zone identification	Op	Op	M	M
Tamper condition	Op	M	M	M
Individual intrusion detector identification (see 8.5.4)	Op	Op	M	M
Zone/Intrusion detector/Hold-up device inhibited	Op	M	M	M
Zone/Intrusion detector/Hold-up device Isolated	Op	M	M	M
Detector(s) fault	Op	Op	M	M
Hold-up device(s) fault	Op	Op	M	M
Prime power source fault	Op	Op	M	M
Alternative power source fault	Op	Op	M	M
Interconnections fault	Op	M	M	M
ATS(s) fault	Op	M	M	M
Warning device(s) fault	Op	M	M	M
Other faults	Op	Op	Op	Op
Overriding of prevention of setting conditions	Op	M	M	M
Detector first to alarm	Op	M	M	M

Events	Grade 1	Grade 2	Grade 3	Grade 4
Battery change required [a]	Op	Op	M	M
Zone/Detector overridden	Op	M	M	M
Changes to time and date	Op	Op	M	M
Changes to site specific data	Op	Op	M	M
Addition/deletion of level 2 users by level 3 user	Op	M	M	M
Detection of substitution (8.7.3)	Op	Op	Op	M
Key: Op = Optional M = Mandatory. NOTE The inclusion of requirements to record events in this table does not imply a requirement to provide the associated function; however, when functions related to the events to be recorded are provided, events arising should be recorded as required by this table.				
[a] Only applicable to primary cells.				

9 Power supply

9.1 Types of power supply

Power supplies included in I&HAS shall comply with the requirements of EN/TS 50131-6 at the appropriate grade and environmental class:

Type A: A prime power source, e.g. mains supply, and an alternative power source recharged by an I&HAS, e.g. a rechargeable battery, automatically recharged by an I&HAS.

Type B: A prime power source and an alternative power source not recharged by an I&HAS, e.g. a battery, not automatically recharged by an I&HAS.

Type C: A prime power source with finite capacity, e.g. a battery.

NOTE Where the prime power source has finite capacity (e.g. a battery), the power supply is considered to be of type C.

9.2 Requirements

The power supply shall be capable of supporting the I&HAS in all conditions including when recharging storage devices within the periods specified in Table 24. The power supply may be placed in one or more I&HAS components or in a separate housing.

A change over between the prime power source and the alternative power source and back again, shall not create an alarm condition, or otherwise influence the status of an I&HAS.

In all grades of I&HAS having a type C power supply as the prime power source, the prime power source shall be capable of powering the I&HAS for a minimum of one year, in all the conditions of use. Type C power supply shall generate a fault signal or message before the voltage falls below the level required for the normal functioning of an I&HAS.

In all I&HAS, using type A or B power supplies, in case of failure of the prime power source, the alternative power source shall be capable of powering an I&HAS for the periods specified in Table 23.

During the periods specified in Table 23, the power supply shall be capable of providing the power required for normal functioning of an I&HAS, including sufficient power to ensure the generation of all mandatory indications and notifications resulting from the processing of two separate intruder alarm signals or messages.

Table 23 – Minimum duration of alternative power supply

Types of power supply	Grade 1 h	Grade 2 h	Grade 3 h	Grade 4 h
Type A	12	12	60	60
Type B	24	24	120	120

In grades 3 & 4 I&HAS, when a prime power source fault is notified to an alarm receiving centre or other remote centre, the duration the alternative power supply may be halved.

NOTE 1 Notification of prime power supply fault may be delayed for a maximum of 1 h as specified in 8.6.

For type A and B power supplies when a supplementary prime power source, with automatic change over between the prime power source and the supplementary prime power source is provided, the period the alternative power source is required to power the I&HAS may be reduced to 4 h.

In all grades of I&HAS an indication, in accordance with the requirements of 8.5, shall be provided when the voltage available from the alternative power source falls below the level required for an I&HAS to operate correctly.

NOTE 2 The actual voltage at which the indication is provided does not have a direct relationship to the period the alternative power source is capable of supporting an I&HAS.

In I&HAS including a type A power supply, the alternative power source shall be recharged to provide 80 % of maximum capacity within the periods specified in Table 24.

Table 24 – Alternative power supply – Recharge periods

Type APS	Grade 1 h	Grade 2 h	Grade 3 h	Grade 4 h
Maximum time to recharge	72	72	24	24

10 Operational reliability

10.1 General

Means shall be provided to ensure that operator errors which might adversely influence the normal operation of an I&HAS are either prevented or indicated.

10.2 I&HAS components

Components of an I&HAS used during the functioning operation of an I&HAS shall be clearly and unambiguously marked and logically arranged in such a manner as to minimise the possibility of incorrect operation. Only those functions accessible at the users access level shall be made available to the user.

11 Functional reliability

I&HAS components shall comply with relevant standards. The design and the configuration of an I&HAS shall ensure the I&HAS functions in accordance with the requirements of this standard. This shall be achieved by

- clear rules for design and installation,
- clear rules for adjustment and maintenance,

- correct manufacture,
- regular maintenance,
- designed to provide a high signal-to-noise ratio,
- well designed software,
- elements working within design limits (voltage, temperature),
- testability of functions (by user, installer),
- function monitoring, e.g. a watchdog circuit.

12 Environmental requirements

12.1 General

The environmental stability of I&HAS shall be of the same level in all grades. The functioning of an I&HAS shall not be influenced when the I&HAS is subject to the environmental conditions specified in Clause 7 and when exposed to EMC conditions specified in 12.2. An I&HAS shall neither change state, suffer damage to components or substantially change in performance. IEC 62599-1 describes environmental test methods which shall be applied to I&HAS components.

12.2 Electromagnetic compatibility

The electromagnetic compatibility performance requirements for I&HAS components are described in IEC 61000-6-3 and IEC 62599-2.

13 Electrical safety

An I&HAS component shall provide protection against electrical shock and consequential hazards by achieving compliance with the requirements of IEC 60950-1 or IEC 60065.

14 Documentation

14.1 Intruder and hold-up alarm system documentation

Documentation relating to an I&HAS shall be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain an I&HAS.

Instructions relating to the operation of an I&HAS shall be designed to minimise the possibility of incorrect operation and be structured to reflect the access level of the user.

14.2 Intruder and hold-up alarm system component documentation

Documentation relating to I&HAS components shall be concise, complete and unambiguous. The documentation shall be sufficient to ensure the correct installation, putting into operation and maintenance of I&HAS components. Sufficient information shall be provided to ensure the integration of each component with other I&HAS components.

Component documentation shall include the following:

- name of manufacturer or supplier;
- description of equipment;
- standard to which component claims compliance;

- name[2] or mark of the certification body;
- security grade;
- environmental class.

15 Marking/Identification

All I&HAS components shall be marked with the following:

- name of manufacturer or supplier;
- type;
- date of manufacture or batch number or serial number;
- standard to which the component claims compliance;
- security grade;
- environmental class.

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

2 If certified.

Annex A
(normative)

Special national conditions

Special national condition: National characteristic or practice that cannot be changed even over a long period, e.g. climatic conditions, electrical earthing conditions.

NOTE If it affects harmonization, it forms part of the European Standard.

For the countries in which the relevant special national conditions apply, these provisions are normative, for other countries they are informative.

Subclause	Special national condition
7.5	**Denmark, Finland, Norway, Sweden**
	Environmental Class IV – Outdoor – General
	Replacement:
	I&HAS components shall function correctly when exposed to environmental influences normally experienced out of doors when an I&HAS components are fully exposed to the weather.
	Temperatures may be expected to vary between –40 °C and +60 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year, relative humidity can be expected to vary between 85 % and 95 % non-condensing.

Annex B
(informative)

Alarm transmission system performance criteria

The security classification of an alarm transmission system is defined as the combination of 5 parameters:

D transmission time - classification

T reporting time

M transmission time - maximum values

S substitution security

I information security

The value of these parameters are defined in EN 50136-1-1 and the following tables and in the text "Signalling security" below.

Table B.1 – Transmission time classification

Class	D0 s	D1 s	D2 s	D3 s	D4 s
Arithmetic mean of all transmissions	-	120	60	20	10
Upper 95 % for all transmissions	240	240	80	30	15

Table B.2 – Transmission time – Maximum values

Class	M0 s	M1 s	M2 s	M3 s	M4 s
Maximum acceptable transmission time	-	480	120	60	20

Table B.3 – Reporting time classification

Class/Period	Reporting time					
Class	T1 d	T2 h	T3 min	T4 s	T5 s	T6 s
Maximum period	32	25	300	180	90	20

Signalling security

The alarm transmission system shall provide measures to prevent or detect deliberate attempts to interfere with the transmission of an alarm message or other information transmitted between an I&HAS and its associated alarm receiving centre by blocking or substitution in one of the following ways.

Substitution security: Protection against unauthorised substitution of the alarm system transceiver with similar equipment along the alarm transmission system transmission path shall be provided in one of the following ways:

S0 No measures.

S1 Measures to detect substitution of the supervised premises transceiver by addition of an identity or address in all messages transmitted on the alarm transmission path.

S2 Measures to detect substitution of the supervised premises transceiver by

a) encryption of an identity or address in all messages transmitted on the alarm transmission path,

b) authentication of the supervised premises transceiver by the addition of a different and un-revealed code for each connected transceiver, or

c) another measure as specified by the manufacturer.

Authentication always requires a sufficient number of keys to provide each connected transceiver with a unique code. The identity range in S2 shall not be less than 250 unique addresses.

Information security: Protection of the information transmitted by the alarm transmission system shall be provided in one of the following ways:

I0 No measures.

I1 Measures to prevent unauthorised reading of the information transmitted.

NOTE 1 This may be accomplished by encryption.

I2 Measures to prevent unauthorised modification of the information transmitted.

NOTE 2 This may be accomplished by encryption or by a cryptographic authentication method.

I3 Measures to prevent unauthorised reading and modification of the information transmitted.

Encryption algorithms shall be such that for synchronous alarm transmission systems, the data pattern of any successive 100 bits shall not be repeated within 10 000 000 successive bits, or for asynchronous systems, the data pattern of any successive 100 bytes shall not be repeated within 1 000 000 successive bytes.

Bibliography

IEC 60073:2002, *Basic and safety principles for man-machine interface, marking and identification – Coding principles for indicators and actuators*

EN/TS 50131-7:2008, *Alarm systems – Intrusion and hold-up systems – Part 7: Application guidelines*[3]

———————

3 The transformation of this document as IEC 62642-7 is under consideration.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 1: Exigences système

AVANT-PROPOS

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

La Norme internationale CEI 62642-1 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme et de sécurité électronique.

La présente norme est basée sur l'EN 50130-1 (2006) et son Amendement 1 (2009).

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/280/FDIS	79/299/RVD

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

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

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

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

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

INTRODUCTION

La présente norme est une partie de la série de Normes Internationales et de Spécifications Techniques CEI 62642 "*Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up*", conçue pour comprendre les parties suivantes:

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

La présente Norme Internationale s'applique aux systèmes d'alarme contre l'intrusion et les hold-up (I&HAS)[1]. La norme est également destinée aux systèmes d'alarme contre l'intrusion (IAS)[2] qui contiennent uniquement des détecteurs contre l'intrusion, et aux systèmes d'alarme contre les hold-up (HAS)[3] qui contiennent uniquement des dispositifs contre les hold-up.

La présente Norme Internationale est une spécification destinée aux systèmes d'alarme contre l'intrusion et les hold-up installés dans les immeubles, et comprend quatre grades de sécurité et quatre classes d'environnement.

Le but d'un I&HAS est d'améliorer la sécurité des locaux protégés. Pour rendre maximale son efficacité, il convient que le I&HAS soit intégré aux dispositifs de sécurité physique et aux procédures appropriés. Ceci est particulièrement important pour les I&HAS de grade de sécurité élevé.

La présente norme est conçue pour aider les assureurs, les sociétés d'alarme d'intrusion, les clients et les services de police, en réalisant une spécification complète et précise de la supervision exigée dans des locaux particuliers, mais elle ne spécifie pas le type de technologie, ni l'étendue ou le niveau de détection, pas plus qu'elle ne couvre nécessairement toutes les exigences relatives à une installation particulière.

---

1 I&HAS = *Intrusion and Hold-up Alarm Systems*.

2 IAS = *Intruder Alarm Systems*.

3 HAS = *Hold-up Alarm Systems*.

Toutes les références aux exigences des I&HAS font référence à des exigences minimales de base et il convient que les concepteurs de ces I&HAS installés prennent en compte la nature des locaux protégés, la valeur des contenus, le niveau du risque d'intrusion, la menace pour le personnel et tout autre facteur pouvant influencer le choix d'un grade de sécurité, ainsi que le contenu d'un I&HAS.

Les recommandations de conception, de planification, d'utilisation, d'installation et de maintenance sont données dans le guide d'application EN/TS 50131-7.

La présente norme n'est pas conçue pour être utilisée dans le cadre d'essais de composants individuels de I&HAS. Les exigences relatives à l'essai de composants individuels de I&HAS sont données dans les normes appropriées relatives aux composants.

Les I&HAS et les composants sont de plus classés par grades pour indiquer le niveau de sécurité demandé. Les grades de sécurité prennent en compte le niveau des risques en fonction du type des locaux surveillés, de la valeur de leurs contenus et du profil caractéristique des intrus ou des voleurs envisagés.

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

Partie 1: Exigences système

1 Domaine d'application

La présente partie de la CEI 62642 spécifie les exigences des systèmes d'alarme contre l'intrusion et les hold-up (I&HAS) installés dans les immeubles utilisant des liaisons filaires spécifiques ou non spécifiques, ou des liaisons non filaires. Ces exigences s'appliquent également aux composants d'un I&HAS installé dans un immeuble, normalement fixés sur une structure externe de l'immeuble, ex: des matériels de commande auxiliaire ou des dispositifs d'avertissement. La norme ne contient pas d'exigences pour les I&HAS situés à l'extérieur.

La présente Norme Internationale spécifie les exigences de performance des I&HAS installés, mais elle ne comprend pas d'exigences pour la conception, la planification, l'installation, le fonctionnement ou la maintenance.

Ces exigences s'appliquent aussi aux I&HAS partageant leurs moyens de détection, de déclenchement, de liaison, de commande, de communication et d'alimentation avec d'autres applications. Le fonctionnement d'un I&HAS ne doit pas être influencé défavorablement par d'autres applications.

Les exigences sont spécifiées pour les composants de I&HAS si l'environnement correspondant est classifié. Cette classification décrit l'environnement dans lequel est supposé fonctionner un composant I&HAS tel qu'il est conçu. Si les exigences relatives aux quatre classes d'environnement sont inadaptées en raison de conditions extrêmes rencontrées dans certains emplacements géographiques, des conditions nationales particulières sont données en Annexe A. Les exigences générales relatives à l'environnement concernant les composants des I&HAS sont décrites dans l'Article 7.

Les exigences de la présente norme s'appliquent également aux IAS et HAS lorsque ces systèmes sont installés de façon indépendante.

Lorsqu'un I&HAS ne comprend pas de fonctions relatives à la détection d'intrus, les exigences relatives à la détection d'intrusion ne s'appliquent pas.

Lorsqu'un I&HAS ne comprend pas de fonctions relatives au hold-up, les exigences relatives au hold-up ne s'appliquent pas.

NOTE Sauf indication contraire, l'abréviation I&HAS est destinée aussi à désigner les IAS et HAS.

2 Références normatives

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

CEI 60065:2001, *Appareils audio, vidéo et appareils électroniques analogues – Exigences de sécurité*

CEI 60950-1:2005, *Matériels de traitement de l'information – Sécurité – Partie 1: Exigences générales*

CEI 61000-6-3:2006, *Compatibilité électromagnétique (CEM) – Partie 6-3: Normes génériques – Norme sur l'émission pour les environnements résidentiels, commerciaux et de l'industrie légère*

CEI 62599-1:2010, *Systèmes d'alarme – Partie 1: Méthodes d'essais d'environnement*

CEI 62599-2:2010, *Systèmes d'alarme – Partie 2: Compatibilité électromagnétique – Exigences relatives à l'immunité des composants des systèmes d'alarme de détection d'incendie et de sécurité*

EN/TS 50131-6:2008, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 6: Alimentation*[4]

EN 50136-1-1:1998, *Systèmes d'alarme – Systèmes et équipements de transmission d'alarme – Partie 1-1: Exigences générales pour les systèmes de transmission d'alarme*

3 Termes, définitions et abréviations

3.1 Termes et définitions

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

3.1.1
action
(relative à la mise en surveillance et hors surveillance) toute action délibérée ou tout acte provoqué par l'utilisateur, qui constitue une partie du procédé de mise en surveillance ou hors surveillance

3.1.2
niveau d'accès
niveau d'accès à des fonctions particulières d'un I&HAS

3.1.3
actif
état d'un détecteur en présence d'un risque

3.1.4
période active
période pendant laquelle un signal d'alarme est présent

3.1.5
alarme
avertissement de la présence d'un risque concernant la vie, la propriété ou l'environnement

3.1.6
centre de réception d'alarme
centre distant occupé en permanence, auquel l'information concernant l'état d'un ou de plusieurs I&HAS est reportée

---

4 La transformation de ce document en CEI 62642-6 est à l'étude.

3.1.7
société d'alarme
organisation qui fournit des services pour les I&HAS

3.1.8
condition d'alarme
condition d'un I&HAS, ou d'une partie de celui-ci résultant de la réponse du système à la présence d'un risque

3.1.9
notification d'alarme
passage d'une condition d'alarme à des dispositifs d'alarme et/ou à des systèmes de transmission d'alarme

3.1.10
système d'alarme
installation électrique activée par la détection manuelle ou automatique de la présence d'un risque

3.1.11
systèmes de transmission d'alarme
matériel et réseau utilisés pour transférer des informations d'un ou plusieurs I&HAS vers un ou plusieurs centres de réception d'alarme

NOTE Les systèmes de transmission d'alarme excluent les liaisons locales directes, c'est-à-dire les liaisons entre les parties d'un I&HAS ne nécessitant pas une interface pour transformer les informations de l'I&HAS en une forme adaptée à leur transmission.

3.1.12
signalisation d'alerte
signalisation audible et/ou visuelle, disponible après un accès de niveau 1, lorsqu'un I&HAS est dans l'état hors surveillance, indiquant qu'une (ou plusieurs) autre(s) signalisation(s) est (sont) disponible(s) aux utilisateurs après un accès de niveaux 2, 3, ou 4

3.1.13
source d'alimentation de secours
source d'alimentation capable d'alimenter l'I&HAS système pendant une durée prédéterminée lorsque la source d'alimentation principale n'est pas disponible

3.1.14
matériel de commande auxiliaire
matériel utilisé à des fins de commandes complémentaires

3.1.15
application
système de sécurité électronique

EXEMPLE Alarme sociale, CCTV, contrôle d'accès ou système incendie ou système électrique/ autre que de sécurité électronique tel que le chauffage, la climatisation, l'éclairage.

3.1.16
autorisation
permission pour obtenir l'accès aux diverses fonctions de commande de l'I&HAS

3.1.17
codes d'autorisation
clés mécaniques ou logiques permettant l'accès aux fonctions des I&HAS

3.1.18
disponibilité d'une liaison
condition lorsqu'une liaison est capable de transporter un signal ou un message

3.1.19
substitution de composant
remplacement de composants d'un I&HAS par des dispositifs de substitution empêchant le fonctionnement normalement prévu lors de la conception du I&HAS

3.1.20
communication
transmission de messages et/ou de signaux entre les composants d'un I&HAS

NOTE La transmission d'un signal peut comprendre le maintien permanent d'un courant électrique dans un commutateur ou un relais constituant une interface entre les composants de l'I&HAS. Il n'est pas nécessaire de changer l'état de l'un quelconque de ces commutateurs ou relais. En raison de la nature des échanges de données, la transmission d'un message peut nécessiter une initialisation délibérée, par exemple en réponse à une consultation ou à une consultation à des intervalles de temps déterminés, cette initialisation peut nécessiter, ou ne pas nécessiter le changement d'état d'un commutateur ou d'un relais.

3.1.21
continuellement
d'une manière récurrente, fréquemment à intervalle régulier

3.1.22
équipement de contrôle et de signalisation
matériel pour recevoir, traiter, commander, afficher et initialiser la transmission ultérieure d'informations

3.1.23
chemin d'accès/de sortie
chemin par lequel l'entrée ou la sortie autorisée de la zone surveillée ou de l'une de ses parties peut être réalisée

3.1.24
événement
condition résultant de l'utilisation d'un I&HAS, par exemple mise en surveillance/hors surveillance ou fonctionnement d'un I&HAS, par exemple signal ou message d'alarme

3.1.25
enregistrement d'événement
stockage des événements résultant de l'utilisation, par exemple mise en surveillance/hors surveillance d'un I&HAS ou fonctionnement d'un I&HAS, pour une analyse ultérieure

3.1.26
condition de défaut
condition d'un système d'alarme interdisant à un I&HAS ou à une partie de celui-ci de fonctionner normalement

3.1.27
signal de défaut
message de défaut
information générée due à la présence d'un défaut

3.1.28
système d'alarme contre les hold-up
système d'alarme fournissant les moyens à un utilisateur de provoquer de manière délibérée une condition d'alarme indiquant un hold-up

3.1.29
dispositif contre les hold-up
dispositif qui une fois déclenché provoque la génération d'un signal ou d'un message d'alarme indiquant un hold-up

3.1.30
condition d'alarme hold-up
condition d'un système d'alarme, ou d'une partie de celui-ci, résultant de la réponse d'un I&HAS au déclenchement d'un dispositif contre les hold-up

3.1.31
signalisation
information (sonore, visuelle ou sous toute autre forme) fournie pour assister l'utilisateur dans le fonctionnement d'un I&HAS

3.1.32
inhibition
état d'une partie d'un I&HAS dans lequel une condition d'alarme ne peut pas être notifiée, un tel état étant maintenu jusqu'à ce que l'I&HAS ou une partie de celui-ci passe de l'état en surveillance à l'état hors surveillance

3.1.33
liaison
moyen par lequel des messages et/ou des signaux sont communiqués entre composants d'un I&HAS

3.1.34
supports de liaison
support par lequel les signaux ou les messages transitent

3.1.35
interférences
perturbations des signaux et/ou des messages circulant entre les composants d'un I&HAS

3.1.36
système d'alarme intrusion
système d'alarme pour détecter et indiquer la présence, l'effraction ou la tentative d'effraction d'un intrus à l'intérieur de locaux surveillés

3.1.37
condition d'alarme intrusion
condition d'un I&HAS, ou d'une partie de celui-ci, résultant de la réponse de l'I&HAS à la présence d'un intrus

3.1.38
signal d'intrusion
message d'intrusion
information générée par un détecteur d'intrusion

3.1.39
détecteur d'intrusion
équipement conçu pour générer un signal ou message d'intrusion en réponse à la détection d'une condition anormale indiquant la présence d'un risque

3.1.40
système d'alarme contre l'intrusion et les hold-up
système d'alarme combinant la gestion de l'intrusion et des hold-up

3.1.41
isolation
état d'une partie d'un système d'alarme dans lequel une condition d'alarme ne peut pas être notifiée, un tel état étant maintenu jusqu'à son annulation par un utilisateur

3.1.42
masqué
condition par laquelle le champ de vision d'un détecteur de mouvement est neutralisé

3.1.43
message
ensemble de signaux transportés via des liaisons comprenant l'identification, les données relatives aux fonctions et les différents dispositifs destinés à assurer sa propre intégrité, son immunité et la réception correcte

3.1.44
substitution de message
création délibérée ou non de messages de substitution circulant entre les composants d'un I&HAS interdisant le bon fonctionnement de celui-ci

3.1.45
contrôle
processus destiné à vérifier que les liaisons et les matériels fonctionnent correctement

3.1.46
liaison filaire non spécifique
liaison transportant des informations appartenant à deux applications ou plus

3.1.47
condition normale
état d'un I&HAS dans lequel n'existe aucune condition qui pourrait interdire la mise en surveillance d'un I&HAS

3.1.48
notification
action de transmettre une alarme, une fraude ou une condition de défaut, aux dispositifs d'avertissement et/ou aux systèmes de transmission d'alarme

3.1.49
opérateur
individu (un utilisateur) autorisé à utiliser un I&HAS dans un but intentionnel

3.1.50
dérogation
intervention, par un utilisateur, permettant la mise en surveillance lorsqu'un I&HAS n'est pas dans une condition normale

3.1.51
en surveillance partielle
état d'un I&HAS dans lequel une condition d'alarme intrusion ou une condition d'alarme indiquant un hold-up peut être notifiée mais avec une partie de l'I&HAS hors surveillance

3.1.52
signalisation "en attente"
moyen signalant que davantage d'information est disponible pour affichage lorsque toutes les informations ne peuvent pas être affichées simultanément

3.1.53
communication périodique
tout signal ou message valide

3.1.54
alimentation
partie d'un système d'alarme fournissant l'énergie à un I&HAS ou une partie de celui-ci

3.1.55
source d'alimentation principale
source d'alimentation utilisée pour maintenir un I&HAS en conditions normales de fonctionnement

3.1.56
réarmement
processus d'annulation d'une alarme, de l'autosurveillance, d'un défaut ou d'une autre condition et rétablissant un I&HAS dans sa condition précédente

3.1.57
dispositif auto-alimenté
dispositif incorporant ses propres sources d'alimentation

3.1.58
capteur
partie d'un détecteur captant un changement d'état

3.1.59
en surveillance
état d'un I&HAS ou d'une partie de celui-ci dans lequel une condition d'alarme intrusion ou une condition d'alarme indiquant un hold-up ne peut pas être notifiée

3.1.60
signal
paramètres variables par lesquels des informations sont transportées

3.1.61
réduction significative de portée
réduction de la plage de détection d'un détecteur de mouvement, mesurée sur l'axe central du détecteur, excédant 50 % de la plage spécifiée

3.1.62
données particulières au site
information relative à la configuration d'un I&HAS, ex.: paramètres de traitement

3.1.63
liaison filaire spécifique
liaison transportant des informations appartenant à une seule application

3.1.64
autonomie
durée pendant laquelle la source d'alimentation de secours est capable d'alimenter un I&HAS

3.1.65
sous système
partie d'un I&HAS située dans une zone clairement définie des locaux protégés et pouvant fonctionner indépendamment des autres parties de l'I&HAS

3.1.66
locaux surveillés
partie de bâtiment et/ou secteur dans laquelle une intrusion, une tentative d'intrusion, ou le déclenchement d'un dispositif contre les hold-up peut être détecté par un I&HAS

3.1.67
source d'alimentation principale complémentaire
source d'énergie (indépendante de la source d'alimentation principale) capable d'alimenter un I&HAS pendant une durée complémentaire, sans affecter l'autonomie de la source d'alimentation de secours

3.1.68
composants d'un système
éléments individuels d'un matériel qui, lorsqu'ils sont configurés ensemble, constituent un I&HAS

3.1.69
transmetteur des locaux surveillés[5]
appareil placé dans les locaux surveillés incluant l'interface avec l'I&HAS et l'interface avec le réseau de transmission d'alarme

3.1.70
fraude
ingérence délibérée dans un I&HAS ou une partie de celui-ci

3.1.71
alarme d'autosurveillance
alarme générée par la détection de la fraude

3.1.72
condition d'autosurveillance
condition d'un I&HAS dans lequel une fraude a été détectée

3.1.73
détection de la fraude
détection d'ingérences délibérées dans un I&HAS ou une partie de celui-ci

3.1.74
protection contre la fraude
méthodes ou moyens utilisés pour protéger un I&HAS ou une partie de celui-ci contre des ingérences délibérées

3.1.75
sécurité d'autosurveillance
méthodes ou moyens utilisés pour protéger un I&HAS ou une partie de celui-ci contre des ingérences délibérées et la détection des ingérences délibérées commises à l'encontre d'un I&HAS ou d'une partie de celui-ci

3.1.76
signal d'autosurveillance
message d'autosurveillance
information générée par un détecteur d'autosurveillance

---

5 Les transmetteurs des locaux surveillés sont appelés « Supervised Premises Transceiver » en anglais.

3.1.77
voie de transmission
voie de transmission entre un système d'alarme individuel et son(ses) centre(s) de réception d'alarme

3.1.78
déclenchement
activation délibérée d'un dispositif contre les hold-up

3.1.79
hors surveillance
état d'un I&HAS ou d'une partie de celui-ci dans lequel une condition d'alarme intrusion et/ou indiquant un hold up ne peut pas être notifiée

3.1.80
utilisateur
personne autorisée à utiliser un I&HAS

3.1.81
interface utilisateur
moyens par lesquels un utilisateur utilise un I&HAS

3.1.82
dispositif d'avertissement
dispositif donnant une alarme audible en réponse à une notification

NOTE 1 Un dispositif d'avertissement peut aussi fournir des indications d'alerte.

NOTE 2 Il convient que de telles indications se distinguent facilement de celles relatives à la notification d'une condition d'alarme.

3.1.83
liaison sans fil
liaison transportant des informations entre les composants d'un I&HAS sans utiliser de support physique

3.1.84
zone
zone de locaux surveillés dans laquelle une intrusion, une tentative d'intrusion, ou le déclenchement d'un dispositif contre les hold-up peut être détecté par un I&HAS

NOTE Bien qu'une zone puisse contenir uniquement un détecteur, le terme « zone » n'est pas synonyme d'une seule entrée de détecteur. Une zone peut comprendre n'importe quel nombre de détecteurs. A titre d'exemples de zones, on peut citer: un étage d'un bâtiment; le périmètre d'un bâtiment; une annexe.

3.2 Abréviations

Pour les besoins du présent document, les abréviations suivantes s'appliquent.

ARC – centre de réception d'alarme[6]

ACE – matériel de commande auxiliaire[7]

ATS – système de transmission d'alarme[8]

---

6 ARC = *Alarm Receiving Centre.*

7 ACE = *Ancillary Control Equipment.*

8 ATS = *Alarm Transmission System.*

CIE – équipement de contrôle et de signalisation[9]

HAS – système(s) d'alarme contre les hold-up[10]

IAS – système(s) d'alarme intrusion[11]

I&HAS – système(s) d'alarme contre l'intrusion et les hold-up[12]

WD – dispositif d'avertissement[13]

PS – alimentation[14]

SPT – transmetteur des locaux surveillés[15]

4 Fonctions du système

L'I&HAS doit inclure, comme indiqué dans la configuration de l'I&HAS, les fonctions spécifiées dans la présente norme pour la détection des intrus et/ou déclenchements, le traitement des informations, la notification des alarmes, ainsi que les dispositifs pour faire fonctionner un I&HAS.

Des fonctions complémentaires aux fonctions obligatoires spécifiées dans la présente norme peuvent être incluses dans un I&HAS à condition qu'elles n'influencent pas le bon fonctionnement des fonctions obligatoires.

5 Composants du système

Les composants de l'I&HAS doivent être classifiés suivant les conditions d'environnement et classés suivant leurs caractéristiques.

Les composants de l'I&HAS doivent être compatibles au sein d'un I&HAS et sélectionnés suivant le grade du système et la classification d'environnement appropriée.

Des composants appartenant à d'autres applications peuvent être combinés ou intégrés à l'I&HAS, à condition que les performances des composants de cet I&HAS ne soient pas dégradées.

6 Grade de sécurité

Les I&HAS doivent avoir un grade de sécurité qui déterminera leurs caractéristiques. Le grade de sécurité doit être déterminé parmi les quatre grades possibles, le grade 1 correspondant au plus petit grade et le grade 4 au plus élevé. Le grade d'un I&HAS doit être celui du composant ayant le grade le moins élevé.

Quand un I&HAS est divisé en sous systèmes clairement définis, un I&HAS peut comprendre des composants de différents grades au sein de chaque sous système. Le grade d'un sous système doit être celui correspondant au composant ayant le grade le moins élevé.

---

9 CIE = *Control and Indicating Equipment.*

10 HAS = *Hold-up Alarm System.*

11 IAS = Intruder Alarm System.

12 I&HAS = Intrusion and Hold-up Alarm System.

13 WD = Warning Device.

14 PS = Power Supply.

15 SPT = Supervised Premises Transceiver.

Les composants partagés par plus d'un sous système doivent avoir un grade égal à celui du sous système ayant le grade le plus élevé (ex.: équipement de contrôle et de signalisation / systèmes de transmission d'alarme / dispositifs d'avertissement / alimentations).

Si une fonction fournie est optionnelle pour un grade particulier, les exigences applicables (quand elles sont identifiées) doivent être satisfaites pour le grade auquel cette fonction prétend répondre. S'il n'y a aucune spécification pour le grade en question, alors les exigences pour tout autre grade plus élevé (tel qu'identifié par le fabricant) doivent s'appliquer.

NOTE 1 Afin de guider les prescripteurs ainsi que les responsables de la sécurité des locaux, les grades suivants sont donnés:

Grade 1: Risque faible

Un intrus ou un malfaiteur est supposé posséder des connaissances faibles sur les I&HAS et utiliser une gamme limitée d'outils disponibles facilement.

Grade 2: Risque faible à risque moyen

Un intrus ou un malfaiteur est supposé posséder des connaissances limitées sur les I&HAS et utiliser une gamme générale d'outils et d'instruments portatifs (ex.: un multimètre).

Grade 3: Risque moyen à haut risque

Un intrus ou un malfaiteur est supposé connaître les I&HAS et posséder une gamme complète d'outils et d'appareils électroniques portatifs.

Grade 4: Haut risque

A utiliser si la sécurité prend le pas sur tous les autres facteurs. Un intrus ou un malfaiteur est supposé avoir la capacité ou les moyens de planifier une intrusion ou un hold-up en détail et posséder une gamme complète d'appareils y compris des moyens de substitution pour les composants d'un I&HAS.

NOTE 2 Dans tous les grades de sécurité, le terme "intrus" est destiné à inclure d'autres types de menaces (ex.: le vol ou la menace avec violence physique, qui peuvent influencer la conception d'un I&HAS).

7 Classification de l'environnement

7.1 Généralités

Les composants doivent être prévus pour une des classes d'environnement suivantes. Les exigences pour les essais d'environnement des composants d'un I&HAS sont mentionnées dans les normes individuelles sur les composants. La CEI 62599-1 décrit les méthodes d'essai d'environnement à appliquer aux composants des I&HAS.

NOTE 1 Les classes I, II, III et IV sont classées par ordre de sévérité croissante, donc les composants de classe IV pourront par exemple être utilisés dans les I&HAS de classe III.

Les composants de l'I&HAS doivent fonctionner correctement lorsqu'ils sont exposés à des conditions d'environnement spécifiées en 7.2, 7.3, 7.4 et 7.5. Pour chaque classe, l'information typique ci-dessous est donnée.

NOTE 2 L'Annexe A inclut des conditions nationales particulières pour les pays spécifiés.

NOTE 3 Les conditions d'environnement décrites dans l'Article 7 sont celles pour lesquelles un I&HAS est supposé fonctionner correctement, elles ne sont pas nécessairement celles à utiliser pendant les essais des composants de l'I&HAS.

7.2 Classe d'environnement I – A l'intérieur

Conditions d'environnement rencontrées normalement à l'intérieur, si la température est bien régulée (ex.: dans une propriété résidentielle ou commerciale).

NOTE Les températures sont supposées varier entre +5 °C et +40 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %.

7.3 Classe d'environnement II – A l'intérieur – En général

Conditions d'environnement normalement rencontrées à l'intérieur, si la température n'est pas bien régulée (ex.: dans les couloirs, halls ou escaliers et là où la condensation peut se produire sur les vitres et dans les aires de stockage non chauffées ou dans les entrepôts chauffés de façon intermittente).

NOTE Les températures sont supposées varier entre –10 °C et +40 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %.

7.4 Classe d'environnement III – A l'extérieur – Sous abri ou à l'intérieur avec des conditions extrêmes

Conditions d'environnement rencontrées normalement à l'extérieur et lorsque les composants de l'I&HAS ne sont pas directement exposés aux intempéries ou à l'intérieur avec des conditions environnementales extrêmes.

NOTE Les températures sont supposées varier entre –25 °C et +50 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Durant 30 jours dans l'année, le taux d'humidité relative sans condensation peut varier entre 85 % et 95 %.

7.5 Classe d'environnement IV – A l'extérieur – En général

Conditions d'environnement rencontrées normalement à l'extérieur et lorsque les composants de l'I&HAS sont directement exposés aux intempéries.

NOTE Les températures sont supposées varier entre –25 °C et +60 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Durant 30 jours dans l'année, le taux d'humidité relative sans condensation peut varier entre 85 % et 95 %.

8 Exigences fonctionnelles

8.1 Détection d'intrusion, de déclenchement, de fraude et reconnaissance des défauts

L'I&HAS doit comprendre, comme indiqué dans sa configuration, les moyens de détection des intrus, de déclenchement, de fraude et de reconnaissance des défauts, nécessaires pour satisfaire aux exigences de cette norme.

NOTE Lorsqu'un I&HAS est configuré comme un IAS, ex.: incluant seulement des détecteurs d'intrusion, il n'est pas nécessaire pour le système de fournir la fonctionnalité requise pour un HAS. De même lorsqu'un I&HAS est configuré comme an HAS, il n'est pas nécessaire pour le système de fournir la fonctionnalité requise pour un IAS.

D'autres événements peuvent être détectés à condition que cela ne perturbe pas les exigences obligatoires de détection des intrus, de déclenchement, d'autosurveillance et de reconnaissance des défauts.

8.1.1 Détection d'intrusion

Les détecteurs doivent être appropriés à l'environnement et à l'application et peuvent comprendre plus d'une technologie.

Les détecteurs doivent être conçus et installés de sorte à maximiser la détection de véritables intrusion et minimiser le risque de fausses alarmes.

Un signal ou un message d'intrusion doit être généré durant le temps requis lorsqu'un détecteur d'intrusion a été activé. Ce temps doit être suffisant pour assurer la réalisation de la communication.

8.1.2 Dispositif contre les hold-up – Déclenchement

L'I&HAS doit inclure, selon le cas, des dispositifs contre les hold-up appropriés à l'environnement et à l'application.

Les dispositifs contre les hold-up doivent inclure les moyens pour minimiser la possibilité de déclenchement accidentel.

Un signal ou un message contre les hold-up doit être généré lorsqu'un dispositif contre les hold-up a été activé pendant le temps requis. Ce temps doit être suffisant pour assurer la réalisation de la communication.

8.1.3 Détection contre la fraude

La détection contre la fraude doit être incorporée dans tous les composants d'un I&HAS comme spécifié dans le Tableau 12.

Un signal ou un message d'autosurveillance doit être généré durant le temps requis lorsque l'autosurveillance d'un détecteur a été activée. Ce temps doit être suffisant pour assurer la réalisation de la communication.

8.1.4 Reconnaissance des défauts

Suivant le grade d'un I&HAS, des moyens doivent être prévus pour reconnaître la condition de défaut telle que spécifiée dans le Tableau 1.

Un signal ou un message de défaut doit être généré durant le temps requis lorsqu'un défaut a été présent pendant la durée exigée. Ce temps doit être suffisant pour assurer la réalisation de la communication.

Tableau 1 – Défauts

Défauts	Grade 1	Grade 2	Grade 3	Grade 4
Détecteur(s)	M	M	M	M
Dispositif(s) contre les hold-up	M	M	M	M
Source d'alimentation principale	M	M	M	M
Source d'alimentation de secours	M	M	M	M
Liaisons	M	M	M	M
Système(s) de transmission d'alarme [a]	M	M	M	M
Dispositif(s) d'avertissement	M	M	M	M
Autres défauts [b]	Op	Op	Op	Op
Légende: M = Obligatoire Op = Optionnel NOTE L'exigence pour un I&HAS pour reconnaître les défauts d'un détecteur, d'un dispositif contre les hold-up, d'un ATS et d'un WD n'implique pas que de tels équipements doivent avoir une sortie de défaut spécialisée, par exemple un défaut de WD peut dériver d'une défaillance d'une communication périodique.				
[a] Lorsqu'un I&HAS nécessite par son grade et son option de notification d'avoir plus d'un système de transmission d'alarme, un défaut sur n'importe quel ATS est reconnu. [b] Autres défauts définis dans les normes relatives aux composants.				

8.2 Autres fonctions

8.2.1 Masquage

Pour les grades 3 et 4, les détecteurs de mouvement d'un I&HAS doivent inclure des moyens pour détecter le masquage.

8.2.2 Réduction de la portée du détecteur de mouvement

Pour le grade 4, les détecteurs de mouvement d'un I&HAS doivent inclure des moyens pour détecter une réduction significative de la portée spécifiée.

8.3 Utilisation

Les I&HAS doivent être conçus pour minimiser la possibilité qu'un opérateur puisse générer une fausse alarme.

Les commandes, par exemples les claviers numériques, utilisées durant l'exploitation d'un I&HAS doivent être claires et repérées sans ambiguïté et disposées logiquement de telle sorte que la possibilité de mauvaise manipulation soit minimisée.

8.3.1 Niveaux d'accès

La présente norme spécifie quatre niveaux d'accès utilisateur qui classent par catégories l'aptitude des utilisateurs à accéder aux composants et aux commandes du système.

Les quatre niveaux d'accès sont les suivants.

Niveau 1 Accès à toute personne

Les commandes accessibles au niveau 1 ne doivent comporter aucune restriction d'accès.

Niveau 2 Accès utilisateur, ex.: par un opérateur

Commandes affectant l'état d'utilisation (sans changer la configuration d'un I&HAS, ex.: données particulières au site).

L'accès aux commandes nécessaires pour permettre l'accès au niveau 2 doit être protégé au moyen d'un contact à clé ou actionné à l'aide d'un code ou d'une serrure ou de tout autre moyen équivalent. Les clés ou codes de niveau 2 ne doivent pas permettre l'accès aux niveaux 3 ou 4.

Niveau 3 Accès utilisateur, ex.: par le personnel d'une société d'alarme

Toutes commandes affectant la configuration d'un I&HAS (sans changer la conception du matériel).

L'accès aux commandes nécessaires pour permettre l'accès au niveau 3 doit être protégé au moyen d'un contact à clé ou actionné à l'aide d'un code ou d'une serrure ou de tout autre moyen équivalent. Les clés ou codes de niveau 3 ne doivent pas permettre pas l'accès au niveau 4.

Niveau 4 Accès utilisateur, ex.: par le fabricant de l'équipement

Accès aux composants pour modifier la conception de l'appareil.

L'accès aux commandes nécessaires pour permettre l'accès au niveau 4 doit être protégé au moyen d'un contact à clé ou actionné à l'aide d'un code ou d'une serrure ou de tout autre moyen équivalent.

NOTE L'accès de niveau 4 s'applique lors du changement de la programmation logicielle sans avoir activé un dispositif d'autosurveillance du CEI ou ACE.

L'accès au niveau 3 doit être interdit sauf si

a) l'accès est autorisé par un utilisateur ayant un niveau d'accès 2, ou
b) dans les I&HAS de grades 1, 2 et 3, l'accès au niveau 3 peut être fourni sans autorisation par un utilisateur de niveau 2 à condition que
   1) l'utilisateur auquel on donne accès au niveau 3 se trouve dans les locaux surveillés et ait accès localement au CIE, et

2) l'I&HAS soit mis hors surveillance, et
3) dans l'I&HAS de grade 1, la notification soit donnée par un dispositif d'avertissement lorsque l'accès au niveau 3 est accordé,
4) dans les grades 2 et 3, la notification soit donnée par un dispositif d'avertissement et à distance, c'est à dire par un ATS lorsque l'accès au niveau 3 est accordé.

L'accès au niveau 4 doit être interdit tant qu'il n'a pas été autorisé par un utilisateur de niveau d'accès 2 et par un utilisateur de niveau 3.

L'accès aux niveaux 2, 3 et 4 peuvent être obtenus à distance à condition que l'autorisation, équivalente à celle spécifiée dans le Tableau 3, soit obtenue.

Les fonctions accessibles à chaque niveau sont indiquées dans le Tableau 2.

Tableau 2 – Niveaux d'accès

Fonctions	Niveaux d'accès			
	1	2	3 [a]	4 [b]
Réglage	NP[e]	P	P	NP
Mise hors surveillance	NP	P	P	NP
Réarmement d'un I&HAS	NP	P	P	NP
Vérification des fonctions d'un I&HAS	NP	P	P	NP
Interrogation du journal d'évènements	NP	P	P	NP
Inhibition/Isolation/dérogation [c]	NP	P	P	NP
Ajout/modification des codes d'autorisation individuels	NP	P [d]	P [d]	P [d]
Ajout/suppression des codes et utilisateurs de niveau 2	NP	P	P	NP
Ajout/modification des données particulières au site	NP	NP	P	NP
Modification/remplacement du programme de base	NP	NP	NP	P

Légende: P = Permis NP = Non permis

NOTE 1 L'inclusion des fonctions données dans ce tableau n'implique pas une obligation de la fourniture de telles fonctions d'un I&HAS.

NOTE 2 Ce tableau spécifie les niveaux d'accès pour chaque fonction; les conditions supplémentaires, applicables à chaque fonction, sont spécifiées par ailleurs dans la présente norme.

NOTE 3 Les exigences relatives aux accès utilisateurs ne sont pas destinées à restreindre les méthodes d'initialisation des accès utilisateurs au moment où le CEI est alimenté pour la première fois (par exemple: l'existence de codes d'accès utilisateurs par défaut ou uniques).

[a] Seulement lorsque autorisé au niveau 2.

[b] Seulement lorsque autorisé au niveau 2 et niveau 3.

[c] Dépend du grade.

[d] Un accès individuel est seulement permis pour modifier son propre code utilisateur.

[e] Autorisé seulement dans le grade 1, voir 8.3.4.

8.3.2 Autorisation

La permission d'accéder aux fonctions d'un I&HAS doit être restreinte par l'utilisation de codes d'autorisation ou de moyens équivalents comme cela est indiqué dans le Tableau 3.

Tableau 3 – Exigences relatives aux codes d'autorisation

Niveaux d'accès 2, 3 et 4	Grade 1 différents	Grade 2 différents	Grade 3 différents	Grade 4 différents
Clé logique	1 000	10 000	100 000	1 000 000
Clé mécanique	300	3 000	15 000	50 000
NOTE La référence à des clés logiques et physiques dans le tableau ci-dessus n'exclut pas l'utilisation d'autres moyens d'autorisation, ex.: moyens biométriques.				

8.3.3 Mise en surveillance et mise hors surveillance

Il doit être possible de restreindre l'accès aux moyens de mise en surveillance et hors surveillance pour le ou les utilisateur(s) ayant le niveau approprié d'accès.

Des moyens doivent être fournis pour permettre à l'utilisateur ayant le niveau d'accès approprié de mettre en surveillance et hors surveillance un I&HAS tout en minimisant les possibilités de mises en surveillance incorrectes.

Il est permis de fournir des moyens de mise en et hors surveillance d'un IAS et d'un HAS et/ou de mise en et hors surveillance de parties d'un IAS, HAS ou I&HAS indépendamment.

8.3.4 Réglage

La mise en surveillance d'un I&HAS, ou d'une partie de celui-ci, doit être accomplie par une action autorisée à condition que toutes les fonctions du système, ou d'une partie de celui-ci, soient dans les conditions normales de fonctionnement. Durant la procédure de mise en surveillance, une indication de mise en surveillance peut être fournie.

Les utilisateurs de niveaux d'accès 2 ou 3 sont autorisés à mettre en surveillance les I&HAS, de tout grade, utilisant des codes d'autorisation ou des moyens équivalents tels que spécifiés dans le Tableau 3, grade 1.

L'I&HAS de grade 1 peut être mis en surveillance par des utilisateurs au niveau d'accès 1 (par exemple par un bouton poussoir) à condition que ce processus de mise en surveillance puisse aussi être annulé avant achèvement par un utilisateur au niveau d'accès 1 et que le moyen de mise en surveillance soit situé à l'intérieur des locaux surveillés.

NOTE Il convient que la mise en surveillance du système par des utilisateurs au niveau d'accès 1 soit utilisée avec précaution.

8.3.5 Interdiction de mise en surveillance

La mise en surveillance d'un I&HAS, ou d'une partie de celui-ci, doit être empêchée, à moins d'une dérogation telle que définie en 8.3.6, lorsqu'une ou plusieurs des conditions citées dans le Tableau 4 est présente.

Tableau 4 – Interdiction de mise en surveillance

Interdiction des conditions de mise en surveillance	Grade 1	Grade 2	Grade 3	Grade 4
Détecteur d'intrusion activé [a]	M	M	M	M
Dispositif contre les hold-up activé	M	M	M	M
Détecteur de mouvement masqué	Op	Op	M	M
Réduction de la portée du détecteur de mouvement	Op	Op	Op	M
Défaut de détecteur d'intrusion	Op	M	M	M
Condition d'autosurveillance	Op	M	M	M
Défauts de liaisons	Op	M	M	M

Interdiction des conditions de mise en surveillance	Grade 1	Grade 2	Grade 3	Grade 4
Défaut de source d'alimentation principale	Op	M	M	M
Défaut de source d'alimentation de secours	Op	M	M	M
Défaut du système de transmission d'alarme	Op	M	M	M
Défaut du dispositif d'avertissement	Op	M	M	M
Défauts d'ATS et WD [b]	M	M	M	M
Autres défauts	Op	M	M	M
Légende: M = Obligatoire Op = Optionnel NOTE L'inclusion d'une condition dans ce tableau n'implique pas que la fonction associée est incluse dans un I&HAS.				
[a] Les détecteurs d'intrusion placés sur un chemin de sortie prévu peuvent être exclus. [b] Défauts issus de tout ATS et WD disponibles empêchant toute notification.				

8.3.6 Interdiction de dérogation à la mise en surveillance

Les conditions empêchant la mise en surveillance peuvent faire l'objet de dérogation des utilisateurs dont les niveaux d'accès sont spécifiés dans le Tableau 5. La dérogation doit être limitée à chaque période de surveillance.

La dérogation à l'interdiction des conditions de surveillance doit être enregistrée dans le journal d'évènements.

Il ne doit pas être possible de déroger à une interdiction de condition de surveillance si la dérogation est elle-même le résultat de la génération d'une condition d'alarme.

Tableau 5 – Conditions d'interdiction de dérogation à la mise en surveillance

Interdiction des conditions de mise en surveillance	Grade 1	Grade 2	Grade 3	Grade 4
Détecteur d'intrusion activé [a]	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Dispositif contre les hold-up activé	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Détecteur de mouvement masqué	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Réduction de la portée du détecteur de mouvement	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Défaut de détecteur d'intrusion	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Condition d'autosurveillance	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3	Niveau d'accès 3
Défauts de liaisons	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3	Niveau d'accès 3
Défaut de source d'alimentation principale	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2
Défaut de source d'alimentation de secours	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3
Défaut du système de transmission d'alarme	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3	Niveau d'accès 3
Défaut du dispositif d'avertissement	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3	Niveau d'accès 3
Défauts d'ATS et WD [b]	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3	Niveau d'accès 3

Interdiction des conditions de mise en surveillance	Grade 1	Grade 2	Grade 3	Grade 4
Autres défauts	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 2	Niveau d'accès 3
NOTE L'inclusion des conditions de ce tableau n'implique pas que la fonction associée est fournie.				
[a] Les détecteurs d'intrusion placés sur un chemin de sortie prévu peuvent être exclus.				
[b] Défauts issus de tout ATS et WD disponibles empêchant toute notification.				

8.3.7 Etat en surveillance

Lorsque la procédure de mise en surveillance a été accomplie d'une manière satisfaisante, il doit y avoir pendant un temps limité l'instauration d'une signalisation montrant que le système ou une partie de celui-ci est passé en état en surveillance.

NOTE Il est recommandé que la fin de la signalisation soit d'une durée suffisante pour permettre à un utilisateur de s'assurer de l'état de l'I&HAS.

Pour les I&HAS de grades 1 et 2, lorsqu'un I&HAS ou une partie de celui-ci est en état en surveillance:

a) l'accès aux locaux surveillés ou à une partie de ceux-ci, via un chemin d'entrée/de sortie, doit être empêché, ou

b) l'ouverture de la porte du chemin d'accès/de sortie doit lancer une procédure d'entrée, ou

c) la signalisation de l'état en surveillance/hors surveillance doit être disponible.

Pour les I&HAS de grades 3 et 4, lorsqu'un I&HAS ou une partie de celui-ci est en état en surveillance:

d) l'accès aux locaux surveillés ou à une partie de ceux-ci, via un chemin d'entrée/de sortie, doit être empêché, ou

e) l'ouverture de la porte du chemin d'accès/de sortie doit lancer une procédure d'entrée.

8.3.8 Mise hors surveillance

8.3.8.1 Mise hors surveillance – Généralités

Pour tous les grades, la mise hors surveillance d'un I&HAS ou d'une partie de celui-ci doit être réalisée au moyen d'une action autorisée.

8.3.8.2 Mise hors surveillance (telle que spécifiée au 8.3.7 b))

Lorsqu'un I&HAS ou une partie de celui-ci est mis hors surveillance selon le 8.3.7 b), un chemin depuis l'entrée jusqu'aux moyens de mise hors surveillance doit être défini. La bonne procédure d'entrée accomplie, seuls les détecteurs du chemin d'accès défini doivent être ignorés de façon à permettre l'accès au dispositif de mise hors surveillance.

NOTE 1 La mise hors surveillance en entrant dans la zone surveillée via un chemin d'accès/de sortie est un des moyens de mise hors surveillance. La mise hors surveillance sans entrer dans une zone surveillée est aussi autorisée, autrement dit la mise hors surveillance depuis un endroit situé en dehors de la zone surveillée.

Une période maximale de 45 s doit être autorisée pour accomplir la procédure de mise hors surveillance. Durant cette période, il doit y avoir une indication d'entrée. Si la procédure de mise hors surveillance n'est pas terminée à la fin de la période définie, par exemple après l'expiration de la temporisation d'entrée, une condition d'alarme doit être notifiée. Lorsque la procédure de mise hors surveillance s'est déroulée correctement comme indiqué dans le présent paragraphe, il doit y avoir une indication complète de mise hors surveillance pour montrer que le système ou une partie de celui-ci est passé à l'état hors surveillance. La mise hors surveillance complète doit être signalée durant un maximum de 30 s (voir Tableau 9).

Lorsqu'une condition d'alarme d'intrusion apparaît durant la procédure de mise hors surveillance, la condition d'alarme doit être notifiée par un dispositif d'avertissement ou signalée. Lorsqu'une notification à distance est incluse dans le système d'alarme intrusion, la condition d'alarme ne doit pas être notifiée à distance jusqu'à ce que l'indicateur ou le dispositif d'avertissement ait fonctionné durant un minimum de 30 s et que la temporisation d'entrée ait expiré.

NOTE 2 Lorsqu'un IAS est en procédure de mise hors surveillance, l'indication citée dans l'alinéa ci-dessus n'est pas restreinte par les exigences du Tableau 9.

8.3.9 Restauration

L'I&HAS doit comprendre les moyens nécessaires pour restaurer l'I&HAS, ou une partie de celui-ci, après une condition d'alarme d'intrusion, de hold-up, de fraude ou de défaut. L'accès à ces moyens de restauration doit être restreint aux utilisateurs ayant un niveau d'accès tel que spécifié dans le Tableau 6.

Il est autorisé que tous les grades des IAS puissent être restaurés à distance à condition que les exigences spécifiées en 8.3.1 et 8.3.2 soient respectées et que l'information soit disponible pour déterminer la cause de la condition de restauration.

Tableau 6 – Restauration

	Grade 1	Grade 2	Grade 3	Grade 4
Intrusion	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3
Hold-up	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3
Auto-surveillance	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 3	Niveau d'accès 3
Défaut [a]	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 3	Niveau d'accès 3
Défaut de source d'alimentation principale	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3
Défaut d'ATS	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3
Masquage	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3
Réduction significative de portée	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3	Niveau d'accès 2 ou 3

[a] Excepté les défauts de l'alimentation principale et de l'ATS.

8.3.10 Inhibition

Le système d'alarme intrusion peut comprendre les moyens nécessaires à l'inhibition du fonctionnement de fonctions individuelles ou de groupes de fonctions. L'accès aux moyens d'inhibition doit être restreint aux utilisateurs ayant un niveau d'accès 2 ou 3.

8.3.11 Isolation

L'I&HAS peut inclure les moyens nécessaires pour isoler les fonctions individuelles ou de groupes de fonctions. L'accès aux moyens d'isolation doit être restreint aux utilisateurs ayant les niveaux suivants:

- grades 1 et 2 niveau d'accès 2 ou 3;
- grades 3 et 4 niveau d'accès 3.

8.3.12 Essai

L'I&HAS doit comprendre les moyens pour l'utilisateur, avec accès de niveau 2, de réaliser un essai fonctionnel des détecteurs d'intrusion et du(es) dispositif(s) contre les hold-up, sachant que ces essais ne sont pas destructifs.

8.3.13 Autres fonctions

L'I&HAS peut inclure les moyens nécessaires pour effectuer d'autres utilisations qui ne sont pas spécifiquement inclues dans cette norme.

Les autres utilisations influençant directement ou indirectement les fonctions d'un I&HAS doivent être effectuées par l'utilisateur ayant le niveau d'accès 3.

8.4 Traitement

Le traitement des signaux ou des messages doit dépendre de l'état, du type de signal ou de message et de la configuration de l'I&HAS.

Le Tableau 7 spécifies les exigences pour le traitement des signaux et/ou messages de hold-up, d'intrusion, d'autosurveillance et de défaut.

Les détecteurs individuels peuvent être logiquement regroupés en exigeant la génération d'un ou plusieurs signaux ou messages d'intrusion depuis un ou plusieurs détecteurs d'une condition d'alarme intrusion.

Un détecteur individuel peut être configuré pour exiger plus d'une activation pour générer un signal ou message d'alarme intrusion.

8.4.1 Signaux ou messages d'intrusion

Les signaux et/ou les messages en provenance des détecteurs d'intrusion doivent être traités comme indiqué dans le Tableau 7. Après la notification d'une condition d'alarme, un I&HAS peut rester capable de notifier d'autres conditions d'alarme, dans la mesure où la durée maximale de fonctionnement du WD audible externe est limitée, pour être en accord avec la réglementation locale ou nationale.

NOTE Il convient que les alarmes intrusion multiples, les conditions d'autosurveillance ou de défauts notifiés auprès d'un centre de réception d'alarmes soient traitées de façon à éviter une réponse non souhaitée.

8.4.2 Signaux ou messages contre les hold-up

Les signaux et/ou les messages en provenance des dispositifs contre les hold-up doivent être traités comme indiqué dans le Tableau 7.

Après la notification d'une ou de plusieurs condition(s) d'alarme hold-up, d'autres signaux et/ou messages en provenance des dispositifs contre les hold-up doivent continuer à être traités comme indiqué dans le Tableau 7.

Des signaux et/ou messages multiples en provenance du même dispositif contre les hold-up n'ont pas besoin d'être traités comme indiqué dans le Tableau 7 s'ils apparaissent dans les 180 s qui suivent le signal ou message précédent.

8.4.3 Signaux ou messages d'autosurveillance

Selon le grade de l'I&HAS, un signal ou message de défaut doit être traité comme indiqué dans le Tableau 7.

8.4.4 Signaux ou messages de défaut

Selon le grade de l'I&HAS, un signal ou message de défaut doit être traité comme indiqué dans le Tableau 7.

8.4.5 Signaux ou messages de masquage

Les signaux ou messages de masquage doivent être traités comme des signaux ou messages d'intrusion ou de défaut selon le Tableau 7.

8.4.6 Signaux ou messages de réduction de portée

Les signaux ou messages de réduction de portée doivent être traités comme des signaux ou messages d'intrusion ou de défaut selon le Tableau 7.

Tableau 7 – Traitement des signaux/messages d'alarme d'intrusion, de hold-up, d'autosurveillance et de défaut

		Grade 1				Grade 2				Grade 3				Grade 4			
Etat de l'I&HAS[a]	**Entrées / Sorties**	**Signal/ Message hold-up**	**Signal/ Message intru-sion**	**Signal/ Message d'auto-surveil-lance**	**Signal/ Message de défaut**	**Signal/ Message hold-up**	**Signal/ Message intrusion**	**Signal/ Message d'auto-surveil-lance**	**Signal/ Message de défaut**	**Signal/ Message hold-up**	**Signal/ Message intrusion**	**Signal/ Message d'auto-surveil-lance**	**Signal/ Message de défaut**	**Signal/ Message hold-up**	**Signal/ Message intrusion**	**Signal /Messag e d'auto-surveil-lance**	**Signal/ Message de défaut**
En surveil-lance	Indications	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	Alarme audible externe	Op	M	M	NP	Op	M	M	NP	Op	M	Op	NP	Op	M	Op	NP
	Alarme audible interne	Op	M	M	Op	Op	M	M	Op	Op	M	Op	Op	Op	M	Op	Op
	Type de message ATS	Hold-up	Intrusion	Intrusion ou autosur-veillance	Intrusion ou défaut	Hold-up [b]	Intrusion	Intrusion ou autosur-veillance	Défaut	Hold-up [b]	Intrusion	Autosur-veillance	Défaut	Hold-up [b]	Intrusion	Autosur-veillance	Défaut
Hors surveil-lance	Indications	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	Alarme audible externe	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP
	Alarme audible interne	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP
	Type de message ATS	Op comme hold-up	NP	Op comme autosur-veillance	Op comme défaut	Op comme hold-up	NP	Op comme autosur-veillance	Op comme défaut	Hold-up	NP	Autosur-veillance	Défaut	Hold-up	NP	Autosur-veillance	Défaut

Légende: M = Obligatoire Op = Optionnel NP = Non permis

NOTE 1 La présence dans le présent tableau d'exigences relatives aux dispositifs d'avertissement et aux systèmes de transmission d'alarme n'implique pas que l'I&HAS doit inclure de tels dispositifs ou systèmes; cependant si de tels dispositifs ou systèmes sont inclus dans un I&HAS, ils doivent satisfaire aux exigences du présent tableau.

NOTE 2 Les cellules du tableau contenant Op, M ou NP représentent les sorties des indicateurs, dispositifs d'avertissement et ATS; le fonctionnement de ceux-ci dépend des exigences spécifiées dans les paragraphes relatifs à ces fonctions.

NOTE 3 Même si la spécification d'un élément indique qu'il est obligatoire, lorsqu'une option de notification n'est pas fournie (voir Tableau 10), l'inclusion d'une sortie n'est pas demandée.

NOTE 4 Il est recommandé que les exigences pour l'indication soient lues en complément de celles du 8.5 et que le fonctionnement des indications soit conditionné par les exigences du 8.5.

NOTE 5 Le WD externe ne doit pas être activé par le CEI dans l'état hors surveillance, mais peut s'activer de lui-même suite à l'activation d'une détection de fraude du WD ou d'un défaut de liaisons avec le CEI.

[a] Les signaux et/ou messages doivent fonctionner selon l'état du I&HAS, IAS ou HAS ou une partie de ceux-ci.

[b] Informations relatives à la zone d'alarmes contre les hold-up à inclure dans les informations transmises à l'ARC.

8.5 Indications

8.5.1 Généralités

Les indications spécifiées dans le Tableau 8 doivent être fournies. Lorsqu'une fonction n'est pas incluse dans un I&HAS, les exigences pour les indications associées à cette fonction n'ont pas besoin d'être fournies.

NOTE 1 Comme exemple, lorsqu'un I&HAS n'inclut pas une fonction hold-up, les exigences pour l'indication relative au hold-up n'ont pas besoin d'être fournies.

NOTE 2 Les indications peuvent être supprimées dans certains cas, par exemple pour éviter une indication lors de l'activation d'un dispositif contre les hold-up.

Lorsqu'il n'est pas possible pour les indications de fournir un affichage simultané de toutes les informations disponibles obligatoires, par exemple information obligatoire en attente d'affichage, une indication doit être fournie pour signaler que d'autres informations sont disponibles, ex.: un indicateur "information en attente".

Une indication d'alerte doit être fournie lorsqu'un I&HAS est mis hors surveillance pour indiquer à l'utilisateur qu'il y a des indications en attente.

Tous les indications obligatoires exigées dans cet article doivent être rassemblées au moins en un endroit, dans le CIE ou l'ACE. Des indications supplémentaires peuvent être situées à d'autres endroits.

Lorsque le grade et l'option de notification d'un I&HAS exigent d'avoir plus d'un système de transmission d'alarme, il est recommandé qu'un défaut détecté sur n'importe quel système de transmission soit indiqué à la personne mettant en surveillance le système.

NOTE 3 Les exigences de la CEI 60073 s'appliquent seulement aux indicateurs. Les dispositifs d'avertissement n'ont pas besoin d'être conformes à la CEI 60073.

NOTE 4 La CEI 60073 comporte des exigences relatives à l'utilisation d'indicateurs colorés qui ne sont pas nécessairement à appliquer lorsque la couleur n'est pas utilisée comme un moyen pour différencier les indications, ex.: l'utilisation d'un écran monochrome à cristaux liquides.

Tableau 8 – Indication

Indications	Grade 1	Grade 2	Grade 3	Grade 4
I&HAS en surveillance/Partie en surveillance	M	M	M	M
I&HAS hors surveillance	M	M	M	M
Condition d'alarme hold-up	M	M	M	M
Identification de la zone hold-up	M	M	M	M
Condition d'alarme intrusion	M	M	M	M
Identification de la zone intrusion	M	M	M	M
Indication du détecteur d'intrusion individuel (voir 8.5.4) [a]	Op	Op	M	M
Indicateur de la condition d'alarme du détecteur (voir 8.5.4)	M	M	M	M
Inhibé	M	M	M	M
Isolé	M	M	M	M
Conditions de défaut (voir Tableau 1)	M	M	M	M
Condition d'autosurveillance	M	M	M	M
Masquage (voir 8.2.1)	Op	Op	M	M
Réduction de plage (voir 8.2.2) [d]	Op	Op	Op	M
Indication(s) en attente	M	M	M	M

Indications	Grade 1	Grade 2	Grade 3	Grade 4
Signalisation d'alerte	M	M	M	M
Mise en surveillance (voir 8.3.4) [b]	Op	Op	Op	Op
Fin de la mise en surveillance (voir 8.3.7) [b]	M	M	M	M
Signalisation d'entrée (voir 8.3.8.2) [b, c]	M	M	M	M
Fin de la mise hors surveillance (voir 8.3.8.2) [b, c]	M	M	M	M
Légende: M = Obligatoire Op = Facultatif NOTE Lorsqu'une fonction, ex.: hold-up, n'est pas fournie, la signalisation associée n'est pas demandée.				
[a] L'identification du détecteur individuel s'applique seulement aux détecteurs avec des capacités de traitement, voir 8.5.4. [b] Ces signalisations sont limitées dans le temps. [c] Ces signalisations sont obligatoires seulement lorsque la procédure de mise hors surveillance optionnelle décrite au 8.3.8.2 est utilisée. [d] Peut être la même indication que le masquage.				

8.5.2 Disponibilité des indications

Les indications doivent être disponibles aux utilisateurs au niveau d'accès 1 comme spécifié dans le Tableau 9. Les autres indications mentionnées dans le Tableau 8 doivent être disponibles uniquement aux utilisateurs qui ont accès à un I&HAS aux niveaux d'accès 2, 3 ou 4.

Tableau 9 – Indications disponibles durant l'état en surveillance et hors surveillance avec un niveau d'accès 1

Indications	Grade 1		Grade 2		Grade 3		Grade 4	
	En surveillance	Hors surveillance	En surveillance	Hors surveillance	En surveillance	Hors surveillance	En surveillance	Hors surveillance
I&HAS en surveillance/Partie en surveillance [voir 8.3.7 grades 1 et 2 c)]	Op	NA	Op	NA	NP	NA	NP	NA
I&HAS hors surveillance [voir 8.3.7 grades 1 et 2 c)]	NA	Op	NA	Op	NA	NP	NA	NP
Signalisation d'alerte	NP	M [c]	NP	M [c]	NP	M [c]	NP	M [c]
Mise en surveillance (voir 8.3.4) [a]	NA	Op	NA	Op	NA	Op	NA	Op
Fin de la mise en surveillance (voir 8.3.7) [a]	M	NA	M	NA	M	NA	M	NA
Signalisation d'entrée (voir 8.3.8.2) [a, b]	M	NA	M	NA	M	NA	M	NA
Fin de la mise hors surveillance (voir 8.3.8.2) [a, b]	NA	M	NA	M	NA	M	NA	M
Légende: Op = Facultatif NP = Non permis NA = Non applicable M = Obligatoire. NOTE 1 Pour les I&HAS de grades 3 et 4, il n'est pas acceptable de signaler, au niveau d'accès 1, l'état en surveillance/hors surveillance d'un I&HAS. NOTE 2 Lorsqu'une fonction n'est pas fournie, la signalisation associée n'est pas exigée.								
[a] Ces signalisations sont limitées dans le temps. [b] Ces signalisations sont obligatoires seulement lorsque la procédure de mise hors surveillance optionnelle décrite au 8.3.8.2 est utilisée. [c] Cette signalisation est optionnelle si l'I&HAS est en surveillance de la partie.								

8.5.3 Annulation des indications

Les signalisations, excepté les signalisation limitées dans le temps, spécifiées dans le Tableau 8 doivent rester disponibles jusqu'à effacement par un utilisateur.

NOTE Une indication d'alerte doit être émise lorsqu'un I&HAS est hors surveillance, les autres indications doivent être disponibles aux niveaux d'accès 2 et 3 lorsqu'un I&HAS est en surveillance ou hors surveillance.

Il ne doit pas être possible d'annuler une indication tant que la condition, à l'origine de l'indication, est encore présente.

8.5.4 Indication – détecteurs d'intrusion

Les détecteurs d'intrusion qui incluent des fonctions de traitement doivent avoir des moyens individuels pour l'indication des conditions d'alarme comme spécifié dans le Tableau 8.

Les détecteurs d'intrusion sans fonction de traitement peuvent partager des moyens communs d'indication. Pas plus de 10 détecteurs de la sorte sont autorisés à partager des moyens communs d'indication.

8.6 Notification

Les conditions de hold-up, d'alarme intrusion, d'autosurveillance et de défaut, ainsi que les autres conditions doivent être notifiées par un ATS et/ou un WD audible selon les exigences spécifiées dans les Tableaux 10 et 11. Un I&HAS doit inclure des moyens de notification conformes au moins à une des options dépendantes du grade spécifiées dans le Tableau 10.

La durée de la période opérationnelle d'un WD peut être sujette à variation selon la réglementation locale ou nationale.

La présence d'un WD peut être supprimée, lorsque par exemple d'autres évènements arrivent en même temps tels que l'activation d'un dispositif contre les hold-up.

Selon son grade, lorsqu'un I&HAS possède un système de transmission d'alarme, ce dernier doit se conformer aux exigences de la EN 50136-1-1 et aux exigences de performance spécifiées dans le Tableau 11.

Lorsqu'un I&HAS inclut à la fois un ATS et un WD, il est autorisé de retarder le fonctionnement du WD pour une période n'excédant pas 10 min. Il est autorisé de supprimer la présence du WD fournissant la notification à un centre de réception d'alarme ou à une autre source de réception par un système de transmission d'alarme, qui confirme par un centre de réception d'alarme ou une autre source de réception durant le temps de retard.

Si un défaut est détecté sur la voie de transmission utilisée par le système de transmission d'alarme, tout délai de fonctionnement du WD de ce type doit être annulé automatiquement pourvu qu'un ou des défauts soient détectés sur l'ensemble des lignes de transmission disponibles.

Les WD sonores doivent fonctionner pendant au moins 90 s sauf si une période plus courte est stipulée par une réglementation locale ou nationale. La période maximale de fonctionnement doit être de 15 min sauf si une période plus courte est exigée par une réglementation locale ou nationale.

La notification des défauts d'alimentation principale peut être retardée d'une heure au maximum.

Les moyens de notification peuvent être complétés par des moyens non obligatoires à condition que de tels dispositifs n'influent pas sur le fonctionnement correct des dispositifs

obligatoires, ex.: un réseau commandant une sirène ou un dispositif pour affaiblir le champ de vision (générateur de fumée).

Tableau 10 – Exigences relatives à la notification

Notification Equipement	Grade 1			Grade 2				Grade 3				Grade 4			
	Options			Options				Options				Options			
	A	B	C	A	B	C	D	A	B	C	D	A	B	C	D
WD audible fonctionnant à distance	2	Op	Op	2	Op	Op	Op	2	Op	Op	Op	2	Op	Op	Op
WD audible autonome	Op	1	Op	Op	1	Op	Op	Op	1	Op	Op	Op	1	Op	Op
ATS principal	Op	Op	ATS 1	ATS 2	ATS 2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6
ATS additionnel	Op	Op	Op	Op	Op	ATS 1	Op	Op	Op	ATS 3	Op	Op	Op	ATS 4	Op

Légende: Op = Optionnel.

NOTE 1 Les chiffres du tableau spécifient le nombre de dispositifs d'avertissement sonores à inclure par grade et option.

NOTE 2 ATS 1, ATS 2, etc. réfèrent aux critères de performance comme spécifié dans le Tableau 11.

NOTE 3 Lorsque 2 ATS sont spécifiés, il est recommandé que les voies de transmission soient indépendantes et de technologies différentes, typiquement une ligne de communication terrestre et l'autre sans fil.

NOTE 4 Un SPT peut faire partie de plus d'un ATS.

NOTE 5 Les ATS principaux et supplémentaires doivent satisfaire leurs critères de performance définis lorsqu'ils fonctionnent normalement. Le changement suite à la défaillance de l'ATS principal n'est pas une exigence de la présente norme pour la performance de l'ATS supplémentaire.

Le Tableau 11 spécifie les critères de performance de l'ATS comme indiqué dans le Tableau 10 conformément aux exigences de la EN 50136-1-1.

NOTE 1 L'Annexe B inclut un extrait des exigences de performance spécifiées dans l'EN 50136-1-1.

NOTE 2 La présente norme fait référence aux exigences de performance spécifiées dans l'EN 50136-1-1 mais n'inclut pas les exigences liées à la classification de disponibilités.

Tableau 11 – Critère de performances d'un système de transmission d'alarme

Critère de performance	Temps de transmission classification	Temps de transmission valeurs max.	Temps de reporting classification	Sécurité de substitution	Sécurité des informations
ATS 1	D1	M1	T2	S0	I0
ATS 2	D2	M2	T2	S0	I0
ATS 3	D2	M2	T2	S1	I1
ATS 4	D2	M2	T3	S1	I2
ATS 5	D3	M3	T4	S2	I3
ATS 6	D4	M4	T6	S2	I3

8.7 Sécurité contre la fraude

8.7.1 Protection contre la fraude

Les composants d'un I&HAS doivent comporter les moyens d'empêcher l'accès aux éléments internes de façon à minimiser les risques de fraude. Les exigences concernant la protection

contre la fraude peuvent varier suivant le grade d'un I&HAS et suivant le fait que le composant d'un I&HAS est situé à l'intérieur ou à l'extérieur des locaux surveillés.

Les composants de l'I&HAS situés à l'extérieur des locaux surveillés doivent être équipés de moyens appropriés de protection contre la fraude (ex.: matériels de commande auxiliaire, dispositifs d'avertissement).

Toutes les bornes et tous les moyens de réglage mécaniques et électroniques doivent être situés à l'intérieur des coffrets contenant les composants.

Les coffrets doivent être suffisamment robustes pour éviter un accès non détectable aux éléments internes sans dommage visible.

Les moyens d'accès aux éléments internes de l'équipement de contrôle et de signalisation, aux appareils de commande auxiliaires, aux systèmes de transmission d'alarme et aux dispositifs d'avertissement doivent être robustes et protégés mécaniquement. L'accès normal doit nécessiter l'utilisation d'un outil approprié.

Les moyens d'accès aux éléments internes des détecteurs et des dispositifs contre les hold-up doivent être protégés et l'accès normal doit nécessiter l'utilisation d'un outil.

L'accès aux moyens permettant d'ajuster le champ de vision d'un détecteur doit être rendu inaccessible aux personnes non autorisées.

8.7.2 Détection de fraude

Les composants d'un I&HAS spécifiés dans le Tableau 12 doivent inclure des moyens pour détecter la fraude. Le Tableau 13 spécifie les types de fraude à détecter. L'autosurveillance doit fonctionner dans les deux états, en surveillance et hors surveillance, pour tous les grades.

Les dispositifs de commande auxiliaires étudiés pour une implantation à l'extérieur des locaux surveillés doivent inclure des moyens pour empêcher la substitution du dispositif de commande auxiliaire et/ou des signaux ou messages entre le dispositif de commande auxiliaire et l'équipement de contrôle et de signalisation. Cette exigence peut être ignorée dans la mesure où une telle substitution ne peut pas influencer le bon fonctionnement d'un I&HAS.

Tableau 12 – Détection de la fraude – Composants à inclure

Composants	Grade 1	Grade 2	Grade 3	Grade 4
CIE/ACE[a]/SPT/WD/PS	M	M	M	M
Dispositifs contre les hold-up [a]	Op	M	M	M
Détecteurs d'intrusion [b]	Op	M	M	M
Boîtes de dérivation [c]	Op	Op	M	M
Légende: Op = Facultatif M = Obligatoire				

[a] Il n'est pas demandé que les ACE et les dispositifs contre les hold-up portables soient conformes aux exigences de ce tableau.

[b] On accepte le fait qu'il soit peu pratique de prévoir une détection de la fraude dans les contacts magnétiques ou mécaniques. Toutefois pour certains grades, il peut être nécessaire de protéger contre la fraude les contacts magnétiques activés, en utilisant une source externe magnétique ou électromagnétique.

[c] Pour le grade 3, lorsqu'un I&HAS inclut une protection contre la substitution de signaux ou messages, les boîtes de dérivation n'ont pas besoin d'être dotées de détection de la fraude.

Tableau 13 – Détection de la fraude – Formes de fraudes à détecter

Formes	Grade 1	Grade 2	Grade 3	Grade 4
Ouvert par un moyen normal	M	M	M	M
Retrait du plan de fixation – Composants I&HAS non filaires	Op	M	M	M
Retrait du plan de fixation – Composants I&HAS filaires	Op	Op	M [c]	M
Pénétration d'un WD audible	Op	Op	Op	M [a]
Pénétration d'un CIE/ACE/SPT	Op	Op	Op	M [a]
Ajustement de l'orientation d'un détecteur	Op	Op	M [b]	M [b]
Légende: Op = Facultatif M = Obligatoire				
[a] S'applique au CIE, ACE, SPT ou WD lorsqu'ils se trouvent à l'extérieur des locaux surveillés.				
[b] Lorsque l'ajustement de l'orientation est possible.				
[c] Cette exigence est facultative pour les boîtes de jonction et les contacts d'ouverture (magnétiques).				

8.7.3 Contrôle de substitution

Suivant le grade d'un I&HAS, un contrôle doit être assuré pour détecter la substitution de composants de l'I&HAS. Le contrôle doit être conforme aux exigences du Tableau 14. Lorsqu'un I&HAS est en condition en ou hors surveillance et qu'une substitution est détectée, un signal ou message d'autosurveillance doit être généré.

Tableau 14 – Contrôle de substitution

Exigences de contrôle	Grade 1	Grade 2	Grade 3	Grade 4
Substitution de composants d'un I&HAS	Op	Op	Op	M
Légende: M = Obligatoire Op = Optionnel				

8.7.4 Contrôle de substitution – Exigences de temps de réponse

La substitution de composants d'un I&HAS doit être détectée dans les délais spécifiés dans le Tableau 15.

Tableau 15 – Contrôle de substitution – Temps de réponse

Exigences de contrôle	Grade 1 s	Grade 2 s	Grade 3 s	Grade 4 s
Substitution de composants d'un I&HAS	Op	Op	100 [a]	10
Légende: Op = Optionnel.				
[a] Lorsqu'une détection de substitution est comprise dans le grade de l'I&HAS.				

8.8 Liaisons

8.8.1 Généralités

Les liaisons doivent être appropriées aux besoins et conçues pour fournir des moyens fiables de communication entre les composants de l'I&HAS.

Les liaisons doivent être conçues pour minimiser la possibilité de signaux ou messages retardés, modifiés, substitués ou perdus; les exigences pour cela sont spécifiées dans les paragraphes suivants.

La communication doit être établie entre les composants de l'I&HAS pour vérifier que la communication, nécessaire pour le fonctionnement correct de l'I&HAS, puisse s'accomplir correctement et quand cela est nécessaire (ex.: lorsqu'un signal ou message d'alarme est généré).

Les liaisons doivent être contrôlées de façon à

a) détecter le moment où la disponibilité ne répond plus aux exigences spécifiées en 8.8.2 et 8.8.3 ci-dessous,

b) détecter le délai, la modification, la substitution ou la perte d'un signal ou message tel que spécifié en 8.8.5 ci-dessous.

Lorsque les liaisons fonctionnement normalement, un signal ou message doit être émis depuis la source jusqu'au composant de destination en 10 s.

Lorsque le support de la liaison peut être influencé par l'environnement extérieur aux locaux surveillés, des mesures doivent être prises pour s'assurer que ces signaux ou messages ne peuvent pas être retardés, modifiés, substitués ou perdus comme spécifié dans le Tableau 19.

8.8.2 Disponibilité des liaisons

Les liaisons doivent être disponibles pour fournir des moyens fiables de transport de signaux ou messages.

Lorsque des liaisons sont partagées avec d'autres applications, la disponibilité de la liaison d'un I&HAS doit être suffisante pour répondre aux exigences de la présente norme.

8.8.3 Contrôle des liaisons

Le Tableau 16 spécifie la durée maximum autorisée pour qu'une liaison soit considérée indisponible. Lorsque la durée maximum permise est dépassée, un signal ou un message d'autosurveillance ou de défaut doit être généré comme spécifié dans le Tableau 20. Les exigences spécifiées au 8.8.3 ne s'appliquent pas aux dispositifs portables contre les hold-up, ni aux ACE portables.

Tableau 16 – Indisponibilité maximum des liaisons

	Grade 1 s	**Grade 2** s	**Grade 3** s	**Grade 4** s
Durée maximum autorisée d'indisponibilité	100	100	100	10
NOTE L'exigence ci-dessus est destinée à établir si la communication est possible par surveillance du support de communication à s'assurer s'il est disponible de transmettre un signal ou message. Le contrôle peut prendre la forme d'écoute du brouillage lorsque des techniques radio sont utilisées ou lorsqu'un I&HAS partage un système BUS avec d'autres applications contrôlant qu'une autre application n'a pas pris la commande permanente du BUS.				

Pour les I&HAS de grade 1 et 2, lorsque la durée entre les communications périodiques (voir 8.8.4.1) excède 100 s, le support de la liaison doit être contrôlé pour établir sa disponibilité à transporter des signaux et messages.

8.8.4 Vérification

8.8.4.1 Intégrité de la liaison – Communication périodique

L'intégrité de la liaison doit être continuellement vérifiée à des intervalles n'excédant pas ceux spécifiés dans le Tableau 17. En cas de communication non vérifiée selon le Tableau 17, des signaux ou messages doivent être générés comme suit:

a) lorsqu'une communication ne peut pas être vérifiée à cause d'une condition de défaut indentifiée, un signal ou un message de défaut doit être généré comme indiqué dans le Tableau 20;
b) lorsqu'une communication ne peut pas être vérifiée à cause d'une raison non indentifiée, un signal ou un message de défaut ou d'autosurveillance doit être généré comme indiqué dans le Tableau 20.

Tableau 17 – Intervalles de vérification

	Grade 1 min	**Grade 2** min	**Grade 3** s	**Grade 4** s
Intervalles maximum permis entre signaux ou messages de communication périodique	240	120	100	10

8.8.4.2 Vérification durant la procédure de mise en surveillance

La mise en surveillance d'un I&HAS doit être interdite lorsque la réception du dernier signal ou message de vérification issu d'un composant du système remonte à un moment excédant les temps donnés dans le Tableau 18.

Tableau 18 – Période de temps maximum depuis le dernier signal ou message

	Grade 1 min	**Grade 2** min	**Grade 3** s	**Grade 4** s
Durée maximum après la réception du dernier signal ou message	60	20	60	10

8.8.5 Sécurité de la communication

Les I&HAS de grade 4 doivent inclure les moyens pour détecter le retard, la modification, la substitution ou la perte de tout signal ou message comme indiqué dans le Tableau 19.

La période de temps maximum autorisée pour détecter le retard, la modification, la substitution ou la perte de tout signal ou message ne doit pas excéder celles données dans le Tableau 17 plus 10 s.

En cas de détection de retard, de modification, de substitution ou de perte de tout signal ou message, un signal ou message de défaut ou d'autosurveillance doit être généré comme indiqué dans le Tableau 20.

Tableau 19 – Sécurité des signaux et messages

	Grade 1	**Grade 2**	**Grade 3**	**Grade 4**
Retard, modification, substitution ou perte de signaux ou messages	Op	Op	Op	M
Légende: M = Obligatoire Op = Optionnel.				

8.8.6 Signaux ou messages à générer

Les signaux ou messages, provenant de l'exigence des paragraphes inclus dans le Tableau 20, doivent être générés comme indiqué dans le Tableau 20.

Tableau 20 – Signaux ou messages à générer

Exigences	Grade 1	Grade 2	Grade 3	Grade 4
	Signal ou message	Signal ou message	Signal ou message	Signal ou message
Contrôle des liaisons (8.8.3)	T ou F	T ou F	T	T
Communication périodique (8.8.4.1 a)	F	F	F	F
Communication périodique (8.8.4.1 b)	T ou F	T ou F	T	T
Sécurité de la communication (8.8.5)	T ou F	T ou F	T	T
Légende: T = Autosurveillance F = Défaut. NOTE La génération de signaux ou messages est exigée seulement lorsque c'est obligatoire dans le paragraphe applicable.				

8.9 Caractéristique temporelle des I&HAS

8.9.1 Détection d'intrusion, de fraude, de déclenchement et reconnaissance des défauts – Exigences relatives aux temps de réponse

Les signaux d'intrusion, de hold-up et d'autosurveillance restant actifs pendant plus de 400 ms doivent être traités. Les signaux de défauts présents pendant plus de 10 s doivent être traités.

NOTE Les messages d'intrusion, de hold-up, d'autosurveillance et de défaut n'ont à être présents que pendant la période nécessaire pour s'assurer de leur bonne transmission.

8.9.2 Traitement

Les signaux et/ou messages d'intrusion, de hold-up, d'autosurveillance et de défauts doivent être notifiés dans les 10 s.

8.10 Enregistrement des événements

Suivant le grade d'un I&HAS, les événements spécifiés dans le Tableau 22 doivent être enregistrés.

Les moyens utilisés pour enregistrer les événements obligatoires doivent être protégés contre l'effacement ou l'altération accidentels ou délibérés de leurs contenus.

Les moyens d'enregistrement des événements doivent avoir une capacité répondant aux exigences du Tableau 21. Lorsque la capacité des moyens d'enregistrement est limitée et que l'enregistreur d'événements a atteint sa capacité maximale, les événements ultérieurs peuvent provoquer l'effacement des événements les plus anciens.

Les I&HAS de grades 2, 3 et 4 doivent enregistrer en plus de l'événement, l'heure et la date auxquelles l'événement a eu lieu. L'horodateur doit avoir une précision de ± 10 min par an, à la température nominale de 20 °C.

Les moyens d'enregistrement des événements peuvent être inclus dans les composants d'un I&HAS, ou au centre de réception d'alarme. Lorsque l'enregistrement des évènements est assuré par un ARC ou un autre endroit déporté, une indication doit être fournie si la transmission des évènements a échoué. Les I&HAS de grade 2, 3 et 4 doivent inclure les moyens pour stocker les évènements en attente de transmission. Les moyens d'enregistrement à distance doivent satisfaire aux exigences du Tableau 21.

NOTE Lorsque l'enregistrement des événements est effectué à l'ARC, il convient que les moyens de notification nécessaires soient prévus dans un I&HAS. Il convient que les moyens d'enregistrement des événements au centre de réception d'alarme répondent aux exigences du 8.10.

Pour les grades 3 et 4, la possibilité d'obtenir un enregistrement permanent des événements enregistrés doit être prévue. Cette possibilité n'impose pas nécessairement les moyens de produire cet enregistrement permanent.

Le nombre d'évènements enregistrés à partir de n'importe quelle source particulière doit être limité à au moins trois et au maximum 10 durant n'importe quelle période en surveillance ou hors surveillance.

Tableau 21 – Enregistrement des événements – Mémoire

Capacité et autonomie	Grade 1	Grade 2	Grade 3	Grade 4
Capacité de mémoire – Nombre minimum d'évènements	Op	250 évènements	500 évènements	1 000 évènements
Autonomie minimum de la mémoire après un défaut d'alimentation de l'I&HAS	Op	30 jours	30 jours	30 jours
Légende: Op = Optionnel.				

Tableau 22 – Enregistrement des événements – Evénements à enregistrer

Evénements	Grade 1	Grade 2	Grade 3	Grade 4
Identité de l'utilisateur lors de la mise en/hors surveillance (quand c'est possible)	Op	Op	M	M
En surveillance/Partie en surveillance	Op	M	M	M
Hors surveillance	Op	M	M	M
Condition d'alarme hold-up	Op	M	M	M
Identification de la zone hold-up	Op	Op	M	M
Condition d'alarme intrusion	Op	M	M	M
identification de la zone intrusion	Op	Op	M	M
Condition d'autosurveillance	Op	M	M	M
Indication du détecteur d'intrusion individuel (voir 8.5.4)	Op	Op	M	M
Zone/Détecteur d'intrusion/Dispositif contre les hold-up inhibé	Op	M	M	M
Zone/Détecteur d'intrusion/Dispositif contre les hold-up isolé	Op	M	M	M
Défaut de détecteur(s)	Op	Op	M	M
Défaut de dispositif(s) contre les hold-up	Op	Op	M	M
Défaut de source d'alimentation principale	Op	Op	M	M
Défaut de source d'alimentation de secours	Op	Op	M	M
Défaut de liaisons	Op	M	M	M
Défaut d'ATS(s)	Op	M	M	M
Défaut de dispositif(s) d'avertissement	Op	M	M	M
Autres défauts	Op	Op	Op	Op
Conditions d'interdiction de dérogation à la mise en surveillance	Op	M	M	M
Premier détecteur ayant déclenché l'alarme	Op	M	M	M
Changement de batterie exigé [a]	Op	Op	M	M
Zone/Détecteur dérogé(e)	Op	M	M	M
Modification de l'heure et de la date	Op	Op	M	M
Modifications des données particulières au site	Op	Op	M	M
Ajout/Suppression d'utilisateurs de niveau 2 par utilisateur de niveau 3	Op	M	M	M

Evénements	Grade 1	Grade 2	Grade 3	Grade 4
Détection de substitution (8.7.3)	Op	Op	Op	M
Légende: M = Obligatoire Op = Optionnel. NOTE L'inclusion d'exigences relatives aux évènements enregistrés du présent tableau n'implique pas une exigence à fournir la fonction associée; cependant, quand les fonctions relatives aux évènements à enregistrer sont fournies, il est recommandé que les évènements survenant soient enregistrés comme indiqué dans le présent tableau.				
[a] Applicable seulement aux cellules principales du tableau.				

9 Alimentation

9.1 Types d'alimentation

Les alimentations incluses dans les I&HAS devront satisfaire aux exigences de l'EN/TS 50131-6 avec le grade et la classe d'environnement appropriés:

Type A: Une source d'alimentation principale, ex.: réseau d'alimentation, et une source d'alimentation de secours rechargeable par un I&HAS, ex.: une batterie rechargeable, automatiquement rechargée par un I&HAS.

Type B: Une source d'alimentation principale et une source d'alimentation de secours non rechargeable par un I&HAS, ex.: une batterie, non automatiquement rechargée par un I&HAS.

Type C: Une source d'alimentation principale ayant une capacité finie, ex.: une batterie.

NOTE Lorsque la source d'alimentation principale a une capacité finie (par exemple une batterie), l'alimentation est considérée comme étant de type C.

9.2 Exigences

L'alimentation électrique doit être capable de supporter l'I&HAS dans toutes les conditions y compris quand les dispositifs de stockage se rechargent selon les durées spécifiées dans le Tableau 24. L'alimentation électrique peut être placée dans un ou plusieurs composants de l'I&HAS ou dans un logement séparé.

Un basculement entre la source d'alimentation principale et la source d'alimentation de secours et vice versa ne doit pas créer de condition d'alarme, ou tout autre modification de l'état d'un I&HAS.

Pour tous les grades, les I&HAS ayant une alimentation de type C comme source d'alimentation principale, la source principale doit pouvoir alimenter l'I&HAS durant au minimum une année, pour toutes ses conditions d'utilisation. L'alimentation de type C doit générer un signal ou message de défaut avant que la tension tombe en dessous du niveau requis pour un fonctionnement normal d'un I&HAS.

Dans tous les I&HAS, utilisant des alimentations de type A ou B, en cas de défaut de la source d'alimentation principale, la source d'alimentation de secours doit être capable d'alimenter un I&HAS pendant les périodes spécifiées au Tableau 23.

Durant les périodes spécifiées dans le Tableau 23, l'alimentation électrique doit être capable d'alimenter un I&HAS pour un fonctionnement normal, y compris une alimentation suffisante pour assurer la génération de toutes les indications et notifications obligatoires résultant du traitement de deux signaux ou messages d'alarme intrusion séparés.

Tableau 23 – Durée minimum d'une source d'alimentation de secours

Types d'alimentation	Grade 1 h	Grade 2 h	Grade 3 h	Grade 4 h
Type A	12	12	60	60
Type B	24	24	120	120

Pour les I&HAS de grades 3 et 4, lorsqu'un défaut de source d'alimentation principale est notifié à un centre de réception d'alarme ou à un autre centre distant, la durée, pendant laquelle l'alimentation de secours doit alimenter l'I&HAS, peut être divisée par deux.

NOTE 1 La notification du défaut de la source d'alimentation principale peut être retardée de 1 h au maximum comme indiqué en 8.6.

Pour les alimentations de type A et B, lorsqu'une source d'alimentation principale et une source d'alimentation supplémentaire sont prévues avec basculement automatique entre les deux sources d'alimentation, la durée pendant laquelle l'alimentation de secours doit alimenter l'I&HAS peut être réduite à 4 h.

Dans tous les tous les grades d'I&HAS, une indication, en accord avec les exigences du 8.5, doit être donnée lorsque la tension fournie par la source de secours descend au dessous du niveau nécessaire au bon fonctionnement d'un I&HAS.

NOTE 2 La tension réelle à laquelle l'indication est fournie n'a pas de relation directe avec la durée pendant laquelle la source de secours est capable d'alimenter un I&HAS.

Pour tous les I&HAS incluant une alimentation de type A, la source de secours doit être rechargée pour fournir 80 % de la capacité maximale dans les délais spécifiés au Tableau 24.

Tableau 24 – Source d'alimentation de secours – Temps de recharge

Type APS	Grade 1 h	Grade 2 h	Grade 3 h	Grade 4 h
Temps maximum pour recharger	72	72	24	24

10 Fiabilité d'utilisation

10.1 Généralités

Des moyens doivent être fournis pour s'assurer que les erreurs d'opérateurs pouvant influencer défavorablement le fonctionnement normal d'un I&HAS sont soit évitées, soit indiquées.

10.2 Composants d'un I&HAS

Les composants d'un I&HAS, utilisés pendant le fonctionnement d'un I&HAS doivent être marqués clairement, sans ambiguïté et disposés logiquement de façon à minimiser un mauvais fonctionnement éventuel. Seules les fonctions accessibles au niveau d'accès utilisateur doivent être disponibles à l'utilisateur.

11 Fiabilité fonctionnelle

Les composants de l'I&HAS doivent être conformes aux normes appropriées. La conception et la configuration d'un I&HAS doivent garantir les fonctions de l'I&HAS conformément aux exigences de la présente norme. Cela doit être réalisé par

- des règles claires pour la conception et l'installation,

- des règles claires pour les réglages et la maintenance,
- une fabrication correcte,
- une maintenance régulière,
- une conception conduisant à un bon rapport signal sur bruit,
- un logiciel bien conçu,
- des éléments fonctionnant à l'intérieur des limites de conception (tension, température),
- un moyen pour essayer les fonctions (par l'utilisateur, l'installateur),
- fonction de contrôle, ex.: circuit de chien de garde.

12 Exigences relatives à l'environnement

12.1 Généralités

La stabilité vis à vis de l'environnement d'un I&HAS doit être similaire quels que soient les grades. Le fonctionnement d'un I&HAS ne doit pas être modifié lorsqu'il est soumis aux conditions d'environnement spécifiées dans l'Article 7 et lorsqu'il est exposé aux conditions de CEM spécifiées en 12.2. Un I&HAS ne doit ni changer d'état ni subir de dommages sur les composants, ni changer considérablement de performance. La CEI 62599-1 décrit les méthodes d'essai d'environnement qui doivent être appliquées aux composants des I&HAS.

12.2 Compatibilité électromagnétique

Les exigences de performances vis à vis de la compatibilité électromagnétique pour les composants des I&HAS sont décrites dans la CEI 61000-6-3 et la CEI 62599-2.

13 Sécurité électrique

Un composant d'I&HAS doit assurer la protection contre les chocs électriques et les dangers consécutifs, en étant conforme aux exigences de la CEI 60950-1 ou la CEI 60065.

14 Documentation

14.1 Documentation relative à l'I&HAS

La documentation relative à un I&HAS doit être concise, complète et sans ambiguïté. Des informations suffisantes doivent être fournies pour installer, mettre en surveillance, utiliser et maintenir un I&HAS.

Les instructions relatives au fonctionnement de l'I&HAS doivent être conçues pour minimiser les mauvais fonctionnements possibles, et être structurées pour refléter le niveau d'accès de l'utilisateur.

14.2 Documentation relative aux composants de l'I&HAS

La documentation relative aux composants de l'I&HAS doit être concise, complète et sans ambiguïté. La documentation doit être suffisante pour garantir une bonne installation, la mise en fonctionnement et la maintenance des composants de l'I&HAS. Des informations suffisantes doivent être fournies pour garantir l'intégration de chaque composant avec les autres composants de l'I&HAS.

La documentation d'un composant doit comprendre:

- le nom du fabricant ou du fournisseur;
- la description du matériel;

- la norme à laquelle le composant prétend répondre;
- le nom[16] ou la marque de l'organisme de certification;
- le grade de sécurité;
- la classe d'environnement.

15 Marquage et identification

Tous les composants de l'I&HAS doivent être marqués avec:

- le nom du fabricant ou du fournisseur;
- le type;
- la date de fabrication ou le numéro de lot ou le numéro de série;
- la norme à laquelle le composant prétend répondre;
- le grade de sécurité;
- la classe d'environnement.

Le marquage doit être lisible, durable et sans ambiguïté. Lorsque l'espace pour le marquage d'un composant de l'I&HAS est limité, des codes peuvent être utilisés, dans la mesure où ils sont définis dans la documentation associée au composant. Lorsque l'espace est insuffisant pour des codes, le composant doit inclure des moyens d'identification qui permettent la correspondance avec la documentation en fournissant les informations requises.

16 Si certifié.

Annexe A
(normative)

Conditions nationales particulières

Condition nationale particulière: Caractéristique ou pratique nationale qui ne peut être changée, même sur une longue durée, ex.: condition climatique, conditions de mise à la terre électrique.

NOTE Si cela affecte l'harmonisation, cela constitue une partie de la Norme Européenne.

Pour les pays dans lesquels les conditions nationales particulières et appropriées s'appliquent, ces dispositions sont normatives, pour les autres pays elles sont informatives.

Paragraphe	Condition nationale particulière
7.5	**Danemark, Finlande, Norvège, Suède**
	Classe d'environnement IV – A l'extérieur – En général
	Remplacement:
	Les composants de l'I&HAS doivent fonctionner correctement lorsqu'ils sont soumis aux effets de l'environnement normalement constatés pour l'extérieur dans le cas où des composants d'un I&HAS sont pleinement exposés aux intempéries.
	Les températures sont supposées varier entre –40 °C et +60 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Pendant 30 jours par an, l'humidité relative peut varier entre 85 % et 95 % sans condensation.

Annexe B
(informative)

Critères de performances d'un système de transmission d'alarme

La classification de la sécurité d'un système de transmission d'alarme est définie par la combinaison de cinq paramètres:

D temps de transmission - classification

T temps de reporting

M temps de transmission - valeurs maximum

S sécurité vis à vis de la substitution

I sécurité vis à vis des informations

Les valeurs de ces paramètres sont définies dans la EN 50136-1-1 et dans les tableaux suivants et dans le texte "Sécurité des signalisations" ci-après.

Tableau B.1 – Classification du temps de transmission

Classe	D0 s	D1 s	D2 s	D3 s	D4 s
Moyenne arithmétique de toutes les transmissions	–	120	60	20	10
Supérieur à 95 % pour toutes les transmissions	240	240	80	30	15

Tableau B.2 – Temps de transmission – Valeurs maximum

Classe	M0 s	M1 s	M2 s	M3 s	M4 s
Temps de transmission maximum acceptable	-	480	120	60	20

Tableau B.3 – Classification du temps de reporting

Classe/Durée	Temps de reporting					
Classe	**T1** j	**T2** h	**T3** min	**T4** s	**T5** s	**T6** s
Durée maximum	32	25	300	180	90	20

Sécurité des signalisations

Le système de transmission d'alarme doit disposer de moyens permettant d'empêcher ou de détecter des tentatives délibérées d'ingérence dans la transmission d'un message d'alarme ou d'autres informations transmises entre un système d'alarme intrusion et le centre de réception d'alarme associé, par blocage ou substitution parmi une des façons suivantes.

Sécurité de substitution: La protection contre une substitution non autorisée du transmetteur du système d'alarme intrusion par un équipement similaire sur la voie de transmission du système de transmission doit être assurée d'une des façons suivantes:

S0 Aucune mesure.

S1 Mesures pour détecter la substitution du transmetteur des locaux surveillés par l'ajout d'une identité ou d'une adresse dans tous les messages transmis sur la voie de transmission de l'alarme.

S2 Mesures pour détecter la substitution du transmetteur des locaux surveillés par

a) encryptage de l'identité ou de l'adresse dans tous les message transmis sur la voie de transmission d'alarme,

b) authentification du transmetteur des locaux surveillés par l'ajout d'un code invisible et différent pour chaque transmetteur relié, ou

c) une autre mesure définie par le fabricant.

L'authentification nécessite toujours un nombre suffisant de clés pour donner à chaque transmetteur connecté un code unique. La gamme d'identités dans S2 ne doit pas être inférieure à 250 adresses uniques.

Sécurité des informations: La protection des informations transmises par le système de transmission d'alarme doit être assurée d'une des façons suivantes:

I0 Aucune mesure.

I1 Mesure pour empêcher la lecture non autorisée des informations transmises.

NOTE 1 Cela peut être réalisé par encryptage.

I2 Mesures pour empêcher la modification non autorisée des informations transmises.

NOTE 2 Cela peut être réalisé par encryptage ou par une méthode d'authentification cryptographique.

I3 Mesures pour empêcher la lecture non autorisée et la modification des informations transmises.

Les algorithmes d'encryptage doivent être tels que, pour un système de transmission d'alarme synchrone, l'échantillon de données de 100 quelconques éléments binaires successifs ne doit pas être répété dans les 10 000 000 éléments binaires suivants, ou, pour un système asynchrone, l'échantillon de données de 100 quelconques octets successifs ne doit pas être répété dans les 1 000 000 octets suivants.

Bibliographie

CEI 60073:2002, *Principes fondamentaux et de sécurité pour l'interface homme-machine, le marquage et l'identification – Principes de codage pour les indicateurs et les organes de commande*

EN/TS 50131-7:2008, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 7: Guide d'application*[17]

———————

[17] La transformation de ce document en CEI 62642-7 est à l'étude.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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