

English version

**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

Alarmanlagen -
Einbruch- und Überfallenmeldeanlagen
Teil 1: Systemanforderungen

This European Standard was approved by CENELEC on 2006-04-04. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 79, Alarm systems.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50131-1 on 2006-04-04.

This European Standard supersedes EN 50131-1:1997.

The following dates were fixed

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2007-05-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2009-05-01

This standard is part of the EN 50131 series of European Standards and Technical Specifications “Alarm systems - Intrusion and hold-up systems”, written to include the following parts:

Part 1	System requirements
Part 2-2	Requirements for passive infrared detectors
Part 2-3	Requirements for microwave detectors
Part 2-4	Requirements for combined passive infrared and microwave detectors
Part 2-5	Requirements for combined passive infrared and ultrasonic detectors
Part 2-6	Requirements for opening contacts (magnetic)
Part 2-7 ¹⁾	Intrusion detectors - Glass break detectors
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 ¹⁾	Security fog devices

¹⁾ At draft stage.

Contents

Introduction	5
1 Scope	6
2 Normative references	6
3 Definitions and abbreviations	7
3.1 Definitions	7
3.2 Abbreviations	13
4 System functions	14
5 System components	14
6 Security grading	14
7 Environmental classification	15
7.1 Environmental Class I – Indoor	15
7.2 Environmental Class II – Indoor – General	15
7.3 Environmental Class III – Outdoor – Sheltered	15
7.4 Environmental Class IV – Outdoor – General	15
8 Functional requirements	15
8.1 Detection of intruders, triggering, tampering and the recognition of faults	15
8.2 Other functions	17
8.3 Operation	17
8.4 Processing	22
8.5 Indications	24
8.6 Notification	25
8.7 Tamper security	27
8.8 Interconnections	29
8.9 I&HAS timing performance	31
8.10 Event recording	31
9 Power supply	34
9.1 Types of power supply	34
9.2 Requirements	34
10 Operational reliability	35
10.1 I&HAS components	35
11 Functional reliability	35
12 Environmental requirements	35
12.1 Electromagnetic compatibility	35
13 Electrical safety	36
14 Documentation	36
14.1 Intruder and hold-up alarm system documentation	36
14.2 Intruder and hold-up alarm system component documentation	36
15 Marking/Identification	36
Annex A (normative) Special national conditions	37
Annex B (informative) Alarm transmission system performance criteria	38
Table 1 – Faults	16
Table 2 – Levels of access	18
Table 3 – Authorisation code requirements	18
Table 4 – Prevention of setting	19

Table 5 – Overriding of prevention of setting conditions.....	20
Table 6 – Restoring	21
Table 7 – Processing of intruder, hold-up, tamper alarm and fault signals/messages	23
Table 8 – Indication	24
Table 9 – Indications available during set and unset status at access level 1	25
Table 10 – Notification Requirements.....	26
Table 11 – Alarm transmission system performance criteria	27
Table 12 – Tamper detection – Components to include	28
Table 13 – Tamper detection – Means to be detected	28
Table 14 – Monitoring of substitution.....	28
Table 15 – Monitoring of substitution – Timing	29
Table 16 – Maximum unavailability of interconnections.....	30
Table 17 – Verification intervals	30
Table 18 – Maximum time period from last signal or message	30
Table 19 – Security of signals and messages.....	31
Table 20 – Signals or messages to be generated	31
Table 21 – Event recording – Memory	32
Table 22 – Event recording – Events to be recorded.....	33
Table 23 – Minimum duration of alternative power supply.....	34
Table 24 – Alternative power supply– Recharge periods.....	35
Table B.1 – Transmission time classification	38
Table B.2 – Transmission time – Maximum values	38
Table B.3 – Reporting time classification.....	38

Introduction

This European Standard applies to Intrusion and Hold-up Alarm Systems. The standard is also intended to apply to Intruder Alarm Systems which include only intrusion detectors and to Hold-up Alarm Systems which include only hold-up devices.

This European Standard is a specification for Intrusion and Hold-up Alarm Systems (I&HAS) 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 CLC/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.

1 Scope

This European Standard specifies the requirements for Intrusion and Hold-up Alarm Systems 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 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 operation of an I&HAS shall not be 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 operate 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 European 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 intended to also 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.

CLC/TS 50131-7	2003	Alarm systems – Intrusion systems – Part 7: Application guidelines
EN 50130-4	1995	Alarm systems – Part 4: Electromagnetic compatibility – Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5	1998	Alarm systems – Part 5: Environmental test methods
EN 50131-6	1997	Alarm systems – Intrusion systems – Part 6: Power supplies
EN 50136	series	Alarm systems – Alarm transmission systems and equipment
EN 60065	2002	Audio, video and similar electronic apparatus – Safety requirements (IEC 60065:2001, mod.)
EN 60073	2002	Basic and safety principles for man-machine interface, marking and identification – Coding principles for indicators and actuators (IEC 60073:2002)

EN 60950-1	2006	Information technology equipment – Safety – Part 1: General requirements (IEC 60950-1:2005, mod.)
EN 61000-6-3	2001	Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments (CISPR/IEC 61000-6-3:1996, mod.)

3 Definitions and abbreviations

3.1 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

organisation 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

3.1.10

alarm system

an electrical installation which responds to the manual or automatic detection of the presence of a hazard

3.1.11**alarm transmission systems**

equipment and network used to transfer information concerned with the state of 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**

an 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 system 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 EXAMPLE: heating, air conditioning, lighting

3.1.16 authorisation

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

3.1.17**authorisation codes**

physical 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 operating 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 authorised 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. set/unset

3.1.25

event recording

storage of events arising from the operation of an I&HAS e.g. for 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/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 is unset

3.1.33

interconnection

means by which messages and/or signals are transmitted 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 or 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 manually cancelled

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 operation 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 a fault condition exists

3.1.51

part set

status of a zone 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

3.1.55

prime power source

power source used to support an I&HAS under normal operating conditions

3.1.56

restore

procedure of cancelling 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, as specified in the System Design Proposal (see CLC/TS 50131-7, F.5)

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 part of the supervised premises capable of independent operation

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 attributes**

characteristics of an I&HAS arising out of its design and configuration

3.1.69**system components**

individual items of equipment which make an I&HAS when configured together

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 or 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 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 A warning device may also provide alert indications providing such indications are easily distinguishable from an alarm.

3.1.83

wire-free interconnection

interconnection conveying information between I&HAS components without physical media

3.1.84

zone

assessed area where abnormal conditions may be detected

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

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).

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

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. EN 50130-5 describes 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 7.1, 7.2, 7.3 and 7.4. 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.

7.1 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.

7.2 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.

7.3 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 d per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

7.4 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 d 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	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 shall be recognised.				

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 levels 3 and 4 shall be prevented until access has been permitted by a user with level 2 access. Access at level 4 shall also require authorisation by a level 3 user.

Access at levels 2, 3 & 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	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	NP	P	NP
Add/change site specific data	NP	NP	P	NP
Change/replace basic programme	NP	NP	NP	P
<p>Key: P = Permitted NP = Not permitted.</p> <p>NOTE 1 The inclusion of the functions shown in this table does not imply that provision of such functions in I&HAS is mandatory.</p> <p>NOTE 2 This table specifies access levels for each function; further conditions, applicable to each function, are specified elsewhere in this standard.</p> <p>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)</p> <p>^a Only when authorised at level 2.</p> <p>^b Only when authorised at level 2 and level 3.</p> <p>^c Depending on the grade.</p> <p>^d An individual is only permitted to change his/her own user code.</p>				

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, & 4	Grade 1 differs	Grade 2 differs	Grade 3 differs	Grade 4 differs
Logical key	1 000	10 000	100 000	1 000 000
Physical key	300	3 000	15 000	50 000
NOTE Reference to physical 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.

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
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 the associated function must be 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 the associated functions must be provided.				
^a Intrusion detectors on an agreed exit route may be excluded.				
^b Faults in all available ATE 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 & 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 & 4 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.

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 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 this clause 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 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 operated for a minimum of 30 s and the entry timer has expired.

NOTE 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
Prime power source fault	Access level 2	Access level 2	Access level 2	Access level 2
ATS fault	Access level 2	Access level 2	Access level 2	Access level 2

^a Except prime power and ATS faults.

8.3.10 Inhibit

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

- grades 1 & 2 access levels 2 or 3;
- grades 3 & 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 operation 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 than 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

I&HAS status ^a	Inputs Outputs	Grade 1				Grade 2				Grade 3				Grade 4			
		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
<p>Key: M = Mandatory Op = Optional NP = Not permitted.</p> <p>NOTE 1 The inclusion in Table 7 of requirements relating to warning devices and alarm transmission systems does not imply that I&HAS must include such devices or systems, however if such devices or systems are included in an I&HAS they must comply with the requirements of Table 7.</p> <p>NOTE 2 Cells containing Op, M or NP represent outputs to indicators, warning devices and ATS the operation of which is dependent on requirements specified in clauses relating to those functions.</p> <p>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.</p> <p>NOTE 4 Requirements for indication should be read in conjunction with 8.5.</p> <p>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.</p>																	
<p>^a Signals and/or messages shall be processed according to the status of the I&HAS, IAS or HAS or part thereof.</p> <p>^b Information relating to the Zone of the Hold-Up alarm to be included in the information transmitted to an ARC.</p>																	

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.

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.

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

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 EN 60073 apply only to indicators. Warning devices need not comply with EN 60073.

NOTE 4 EN 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
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)	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	M	M	M	M
Completion of unsetting (see 8.3.8.2) ^b	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.				

8.5.2 Availability of indications

Indication, of the conditions specified in Table 9, shall be available, at access level 1, when an I&HAS is in the set or unset state as specified in Table 9. Indications included in Table 8 shall be available 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 & 2 c)]	Op	NA	Op	NA	NP	NA	NP	NA
I&HAS unset [see 8.3.7 grades 1 & 2 c)]	NA	Op	NA	Op	NA	NP	NA	NP
Alert indication	NP	M	NP	M	NP	M	NP	M
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	M	NA	M	NA	M	NA	M	NA
Completion of unsetting (see 8.3.8.2) ^a	NA	M	NA	M	NA	M	NA	M
Key: Op = Optional NP = Not Permitted NA = Not Applicable M = Mandatory.								
NOTE 1 In grade 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.								

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 an 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 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 operation 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.

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

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

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 and 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/ATS/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 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 grades 1, 2 and 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 ^a	Op	M	M	M
Penetration of audible WD ^b	Op	Op	Op	M
Penetration of CIE/ACE/ATS ^b	Op	Op	Op	M
Detector orientation adjustment ^c	Op	Op	M	M
Key : Op = Optional M = Mandatory.				
^a Wire-free detectors only.				
^b When located outside the supervised premises.				
^c When orientation adjustment is possible.				

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 clauses.

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.

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:

- when communication cannot be verified because of an identified fault condition, a fault signal or message shall be generated as shown in Table 20;
- 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 needs to 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 & 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
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 Table 22 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 Table 22.				
^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 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.

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 operation 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 operation 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 A PS	Grade 1 h	Grade 2 h	Grade 3 h	Grade 4 h
Maximum time to recharge	72	72	24	24

10 Operational reliability

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.

10.1 I&HAS components

Components of an I&HAS 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. 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 operation of the I&HAS according to 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 operating within design limits (voltage, temperature),
- testability of functions (by user, installer),
- function monitoring, e.g. a watchdog circuit.

12 Environmental requirements

The environmental stability of I&HAS shall be of the same level in all grades. The operation 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 12.1. An I&HAS shall neither change state, suffer damage to components or substantially change in performance. EN 50130-5 describes environmental test methods which shall be applied to I&HAS components.

12.1 Electromagnetic compatibility

The electromagnetic compatibility performance requirements for I&HAS components are described in EN 61000-6-3 and EN 50130-4.

13 Electrical safety

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

<u>Clause</u>	<u>Special national condition</u>
---------------	-----------------------------------

7.4	Denmark, Finland, Norway, Sweden
-----	---

Environmental Class IV – Outdoor – General

Replacement:

I&HAS components shall operate 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".

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 percentile 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 unrevealed 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 must 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 This may be accomplished by encryption.
- I2 Measures to prevent unauthorised modification of the information transmitted.
NOTE 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.