

TECHNICAL SPECIFICATION

CLC/TS 50131-3

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

July 2003

ICS 13.310

English version

**Alarm systems –
Intrusion systems
Part 3: Control and indicating equipment**

Systemes d'alarme–
Systemes d'alarme intrusion
Partie 3: Matériel de commande et
d'affichage (Centrale d'alarme)

Alarmanlagen –
Einbruchmeldeanlagen
Teil 3: Melderzentrale

This Technical Specification was approved by CENELEC on 2003-05-19.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Lithuania, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and 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

The text of this Technical Specification 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 CLC/TS 50131-3 on 2003-05-19.

The following date was fixed:

- latest date by which the existence of the CLC/TS
has to be announced at national level (doa) 2003-10-30
-

Contents

	Page
1 Scope.....	6
2 Normative references	6
3 Definitions and abbreviations	7
3.1 Definitions	7
3.2 Abbreviations	12
4 Equipment attributes	12
4.1 General	12
4.2 Functionality.....	12
5 CIE structure	13
6 Security grade	13
7 Environmental requirements	14
7.1 General	14
7.2 Environmental class I: Indoor	14
7.3 Environmental class II: Indoor - General	14
7.4 Environmental class III: Outdoor - Sheltered.....	14
7.5 Environmental class IV: Outdoor - General	14
7.6 Special condition.....	14
7.7 Environmental tests	14
8 Functional requirements	14
8.1 Inputs	14
8.2 Operation	15
8.3 Processing	22
8.4 Indication	25
8.5 Notification outputs	28
8.6 Tamper security (detection/protection).....	29
8.7 Fault.....	30
8.8 Interconnections	31
8.9 Timing.....	31
8.10 Event recording	32
8.11 Power supply	33
9 Electrical safety.....	33
10 Product documentation.....	34
10.1 Installation and maintenance	34
10.2 Operating instructions.....	34
11 Marking and labelling	35
12 Tests	35
12.1 Test conditions	35
12.2 Functional tests	36
12.3 Reduced functional test.....	36
12.4 Functional tests	37
12.5 Access level.....	48
12.6 Authorization requirements.....	49

13 Environmental tests 58

 13.1 General..... 58

 13.2 Environmental test selection..... 59

Annexes

Annex A (informative) Interconnection types 64

Annex B (informative) Example of calculation for code variations..... 66

Annex C (informative) Summary of timing requirements..... 68

Figures

Figure A.1 – Specific wired interconnections 65

Figure A.2 – Non specific wired interconnections 66

Figure A.3 – Wire-free interconnections 66

Tables

Table 1 - Access level to functions and control..... 16

Table 2 - Authorization requirements - Access levels 2, 3, and 4..... 16

Table 3 – Detection of repeated incorrect authorisation codes..... 17

Table 4 - Prevention of setting conditions 18

Table 5 - Overriding of prevention of setting conditions..... 18

Table 6 - Authorisation required to restore conditions 20

Table 7 - Automatic inhibit 20

Table 8 - Manual inhibit..... 21

Table 9 - Processing of intruder, hold-up, tamper alarm and fault signals/messages..... 23

Table 10 - Monitoring of processing..... 24

Table 11– Indication (from Table 4 of EN 50131-1)..... 26

Table 12 – Additional indication in the CIE or ACE..... 27

Table 13 - Notification requirements 28

Table 14 - Tamper protection..... 29

Table 15 - Tamper detection..... 29

Table 16– Tool dimension for tamper detection 30

Table 17– Removal from mounting..... 30

Table 18 - Recognition of fault conditions 30

Table 19 - Interconnection confirmation..... 31

Table 20 - Reduced functional test 37

Table 21 – Functional tests 38

Table 22 – Tests of the processing of hold-up signal or messages 39

Table 23 – Tests of the processing of tamper signal or messages 41

Table 24 – Test of the process monitoring 45

Table 25 – Test of processing of fault signals or messages..... 46

Table 26 – Test of processing of optional functions (non specified in EN 50131-1)..... 48

Table 27 – Test of the access to the functions and controls.....	48
Table 28 – Test for disabling user input during incorrect authorization codes.....	51
Table 29 – Test for generation of tamper during incorrect authorization codes	52
Table 30 – Test of setting procedure	53
Table 31 – Test for unsetting procedure.....	54
Table 32 – Test of Entry Route Procedure	55
Table 33 – Test of exit route procedure.....	56
Table 34 – Test of Event Log.....	57
Table 35 - Environmental test selection.....	59
Table C.1 - Timing table.....	69

1 Scope

This Technical Specification specifies the requirements, testing procedures security and environmental performance criteria for control and indicating equipment (CIE) intended for use in intrusion alarm system (IAS) and hold-up alarm systems (HAS) installed in buildings.

This Technical Specification specifies the requirements for CIE installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to the components of a CIE which are normally mounted on the external structure of a building. (EXAMPLE: Ancillary control equipment).

This Technical Specification specifies performance requirements for CIE but does not include requirements for design, planning, installation, operation or maintenance.

These requirements apply also to CIE sharing means of detection, interconnection, control, communication and power supplies with other applications.

Requirements are specified for CIE components where the relevant environment is classified. This classification describes the environment in which the CIE 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 of EN 50131-1. General environmental requirements for CIE components are described in Clause 7.

NOTE In this Technical Specification reference to the term "I&HAS" is used throughout the specification. The term is intended to include IAS and HAS when such systems are installed separately.

2 Normative references

This Technical Specification incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Technical Specification only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

<u>Publication</u>	<u>Year</u>	<u>Title</u>
EN 50130-4	1996	Alarm systems - Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5	1998	Alarm systems - Environmental test methods
EN 50131-1	1997	Alarm systems - Intrusion systems - General requirements
EN 50131-6	1997	Alarm systems - Intrusion systems - Power supplies
EN 60065	2002	Audio, video and similar electronic apparatus – Safety requirements
EN 60529	1991	Specification for degrees of protection provided by enclosures (IP code)
EN 60950	2001	Information technology equipment – Safety – General requirements

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

3 Definitions and abbreviations

For the purposes of this specification, the following definitions and abbreviations apply.

3.1 Definitions

3.1.1

acknowledge

action of a user to accept an indication

3.1.2

action

any deliberate operation or act by the user

3.1.3

active period

period during which an alarm signal is present (See Annex A)

3.1.4

alarm

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

3.1.5

alarm condition

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

3.1.6

alarm notification

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

3.1.7

alarm point

one or more detector(s) grouped together for the purpose of indication or processing

3.1.8

alarm receiving centre (ARC)

continuously manned remote centre to which the information concerning the state of one or more alarm systems is reported

3.1.9

alarm signal

signal generated by a detection device

3.1.10

alarm system

electrical installation which responds to the manual hold-up or automatic detection of the presence of a hazard

3.1.11

alarm transmission system (ATS)

system used to transfer information between one or more alarm systems and one or more alarm receiving centres

3.1.12**alternative power source (APS)**

power source capable of powering the system for a predetermined time when a prime power source (PPS) is unavailable

3.1.13**ancillary control equipment (ACE)**

equipment used for supplementary control purposes

3.1.14**conditioning**

exposure of a specimen to environmental conditions in order to determine the effect of such conditions on the specimen

3.1.15**control and indicating equipment (CIE)**

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

3.1.16**detector**

device designed to generate an alarm signal in response to the sensing of an abnormal conditions indicating the presence of a hazard

3.1.17**entry route facility**

means to ignore signals or messages from specified detectors during unsetting for a specified time period

3.1.18**event recording**

storage of events arising from the operation of the I&HAS components

3.1.19**exit route facility**

means to ignore signals or messages from specified detectors during setting for a specified period

3.1.20**external power source (EPS)**

energy supply external to the IAS which may be non-continuous, used as the prime power source in type A and type B power supply

3.1.21**fault condition**

condition of an alarm system which prevents the system or parts thereof from functioning normally

3.1.22**fault signal or message**

information generated due to the presence of a fault

3.1.23**hold-up alarm system (HAS)**

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

3.1.24

hold-up device

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

3.1.25

indication

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

3.1.26

inhibit

status of a part of an alarm system in which an alarm condition cannot be notified, such status is cancelled when the CIE is unset (EXAMPLE: intruder alarm, tamper alarm, etc.)

3.1.27

interconnections

means by which signals and/or messages are transmitted between I&HAS components

3.1.28

intruder alarm condition

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

3.1.29

intruder detector

device that generates an alarm condition in response to intrusion or attempted intrusion, or to deliberate action by the subscriber

3.1.30

intrusion

entry into the protected premises by an unauthorised person(s)

3.1.31

intrusion and hold-up alarm system (I&HAS)

combined intruder and hold-up alarm system

3.1.32

isolation

status of a part of an alarm system in which an alarm condition cannot be notified, such status remains until deliberately cancelled (EXAMPLE: intruder alarm, tamper alarm, etc)

3.1.33

logical key

code (EXAMPLE: numeric or alphabetic) entered by an authorized user to gain access to restricted functions or parts of a CIE

3.1.34

message

series of signals routed by a network which includes identification, functional data and the means to provide its own integrity, immunity and proper reception

3.1.35

monitoring

process of verifying that the interconnections and equipment are functioning correctly

3.1.36**normal condition**

state of an I&HAS where no conditions exist which would prevent the setting of the system

3.1.37**notification**

passing of alarm, tamper, hold up or fault conditions to warning devices and/or alarm transmission systems

3.1.38**operating mode**

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

3.1.39**override**

intervention by a user to permit setting when a fault condition exists

3.1.40**physical key**

implement used by an authorised user to gain access to restricted functions or parts of a CIE (mechanical key, magnetic card, electronic token or similar)

3.1.41**power supply (PS)**

device that stores, provides and also modifies or isolates (electrical) power for an alarm system or part thereof. The two basic parts of a PS are the Power Unit (PU) and the storage device (EXAMPLE: battery)

3.1.42**power unit (PU)**

device that provides and also modifies or isolates (electrical) power for an IAS or part thereof, and for the storage device if required

3.1.43**prime power source (PPS)**

power source used to support the I&HAS or part thereof under normal operating conditions

3.1.44**restore**

procedure of cancelling an alarm, tamper, fault or other condition and returning the I&HAS to the previous condition

3.1.45**set**

status of an alarm system or part thereof in which an alarm condition can be notified

3.1.46**signal**

variable parameters by which information is conveyed

3.1.47**soak**

an attribute of a zone or alarm point such that signals or messages that normally create notifications are prevented from doing so, but continue to be recorded in the event log. The soak attribute can be manually or automatically removed

3.1.48

stand-by period

defined time for which a power supply shall supply energy to the components of the alarm system in the event of failure of the EPS

3.1.49

storage device

device which stores energy (EXAMPLE: a battery)

3.1.50

storage failure

inability of a storage device to maintain the output voltage above the minimum value, in the event of a failure of the EPS

3.1.51

supervised premises

that part of a building in which a hazard may be detected by an alarm system

3.1.52

tamper alarm

alarm generated by tamper detection

3.1.53

tamper condition

condition of an alarm system, resulting from the detection of tampering

3.1.54

tamper detection

detection of deliberate interference with an alarm system or part thereof

3.1.55

tamper protection

methods or means used to protect an alarm system or part thereof against deliberate interference

3.1.56

test condition

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

3.1.57

triggering

deliberate operation of a hold-up device

3.1.58

unset

status of an IAS or part thereof in which an intruder alarm condition cannot be notified

3.1.59

user

person authorised to operate an alarm system

3.1.60

user input

command generated by a deliberate user action

3.1.61**warning device**

device that gives an alarm or an alert

3.1.62**wire-free interconnection**

interconnection conveying information between I&HAS components without physical media. The interconnection may convey information pertaining to two or more applications

3.1.63**zone**

an assessed area where abnormal conditions may be detected

3.2 Abbreviations

3.2.1 ACE: Ancillary control equipment

3.2.2 APS: Alternative power source

3.2.3 ARC: Alarm receiving centre

3.2.4 ATE: Alarm transmission equipment

3.2.5 ATS: Alarm transmission system

3.2.6 CIE: Control and indicating equipment

3.2.7 EPS: External power source

3.2.8 HAS: Hold-up alarm systems

3.2.9 IAS: Intrusion alarm system

3.2.10 I&HAS: Intruder and hold-up alarm system

3.2.11 PIN: Personal identity number

3.2.12 PPS: Prime power source

3.2.13 PS: Power supply

3.2.14 PU: Power unit

3.2.15 SD: Storage device

3.2.16 WD: Warning device

4 Equipment attributes**4.1 General**

Control and indicating equipment shall include attributes for the detection of input status, processing the information, notification and indication as appropriate. The detailed requirements for the following attributes are provided in Clause 8.

4.2 Functionality

Control and indicating equipment shall include the following functions:

4.2.1 Inputs

The ability to receive and recognize intrusion, tamper and fault signals or messages. Other signals and messages can be received and recognized. Such inputs shall not affect any mandatory requirements of this specification.

4.2.2 Operation

The operation function is to enable the CIE to respond to automatic or manual user instructions (EXAMPLE: set, unset, inhibit, isolate).

4.2.3 Processing

The processing function is to enable the CIE to process signals and messages from detectors and hold-up devices, to process tamper and monitoring functions and respond to user instructions.

4.2.4 Outputs

To give information to the user and to provide notification and/or indication of alarm or fault or tamper conditions.

4.2.5 Tamper security

To enable the CIE to resist tampering using physical means and to provide electrical, electronic or other means to detect tampering.

4.2.6 Monitoring

To monitor, according to the grade, that the CIE and the interconnections are operating correctly.

In the event of a fault condition being detected, the CIE shall provide an indication and/or notification.

5 CIE structure

The CIE can be distributed in multiple housings or be in a single housing, and may be combined with other IAS components.

Other applications or functions not specified in this specification may be provided; such applications or functions shall not affect any requirements given within this specification.

6 Security grade

The CIE requirements shall be divided into four security grades, with grade 1 being the lowest and grade 4 being the highest.

The requirements for the performance of the CIE will vary depending upon its stated grade and will be tested according to the grade in the CIE documentation and marking.

Security grades 1 to 4 shall be in accordance with the descriptions in EN 50131-1.

7 Environmental requirements

7.1 General

Environmental classes I to IV shall be in accordance with the description in EN 50131-1.

To ensure the correct application of I&HAS components, the CIE and the ACE shall be suitable for use in one of the following environmental classes.

7.2 Environmental class I: Indoor

The CIE and ACE shall operate correctly when exposed to environmental influences normally experienced indoors when the temperature is well maintained. (EXAMPLE: in a residential or commercial property).

7.3 Environmental class II: Indoor - General

The CIE and ACE shall operate correctly when exposed to environmental influences normally experienced indoors when the temperature is not well maintained. (EXAMPLE: in corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent).

7.4 Environmental class III: Outdoor - Sheltered

The CIE and ACE shall operate correctly when exposed to environmental influences normally experienced out of doors when the CIE and the ACE are not fully exposed to the weather.

7.5 Environmental class IV: Outdoor - General

The CIE and ACE shall operate correctly when exposed to environmental influences normally experienced out of doors when the CIE and the ACE are fully exposed to the weather.

7.6 Special condition

EN 50131-1, Annex A lists those countries with special environmental conditions.

7.7 Environmental tests

Tests and severity levels are specified in Clauses 12 and 13 of this specification. Environmental test methods are specified in EN 50130-5.

8 Functional requirements

8.1 Inputs

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

8.1.1 Intruder detection

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

8.1.2 Hold-up device

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

8.1.3 Tamper

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

8.1.4 Fault

The CIE shall provide the means to receive and process fault signals or messages.

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

8.1.5 Monitoring (input)

Means shall be provided to verify that the CIE and the interconnections are functioning correctly as defined in 8.3.3 and 8.8 of this specification. The CIE shall provide the means to receive and process monitoring signals or messages. These signals or messages shall be processed as tamper or a fault signals or messages according to Table 9.

NOTE This assumes that an interconnection function is provided (to be specified in EN 50131-5) which generates monitoring signals or messages.

8.1.6 User input

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

8.1.7 Other

When a CIE receives and processes signals or messages or other information not necessary to meet the requirements of this Technical Specification (EXAMPLE: technical monitoring), this shall not affect the ability of the CIE to meet the requirements of this specification.

8.2 Operation

The CIE shall provide the means necessary to enable authorized users to access the functions of the CIE. Access to these functions shall be restricted, (EXAMPLE: by using a keypad or lock).

8.2.1 Access levels

Up to four access levels shall be provided to the functions of a CIE. The functions and permitted access levels are specified in.

If the CIE includes security functions additional to those listed in Table 1 the access levels necessary to operate those functions shall be specified by the manufacturer. Any non-security functions shall be specified in the manufacturer's documentation.

- Level 1 access to any person

NOTE 1 As no authorization requirements exist for access level 1, some indications may appear without user intervention

- Level 2 access to any user
- Level 3 access to service personal
- Level 4 access to manufacturer

Table 1 – Access level to functions and control

Function and controls	Access levels			
	1	2	3*	4*
Indications	P	P	P	P
Set	NP	P	P	NP
Unset	NP	P	P	NP
Restore IAS	NP	P	P	NP
Verify IAS functions	NP	P	P	NP
Interrogate event log	NP	P	P	NP
Inhibit/isolate/override	NP	P	P	NP
Add/change authorisation codes	NP	P **	P **	P **
Add/change site specific data	NP	NP	P	NP
Change the program	NP	NP	NP	P
NP = Not permitted * = Only when authorised by level 2 P = Permitted ** = Only change his own authorisation code, except "master user"				

NOTE 2 In all grades, one or more master user may exist.

Access at levels 3 and 4 shall be authorized by access level 2 in one of two ways:

- access remains authorized until manually removed;
- authorization is required each time.

It is permitted to have the access levels sub-divided into a table of rights provided by the manufacturer to operate the available functions.

Means shall be provided to prevent reading of authorization codes.

NOTE 3 Access level 4 applies when changing the operating programme software without having activated a tamper device on the CIE or ACE

8.2.2 Authorization

Access to the functions of a CIE (as defined) at levels 2, 3 and 4 shall be restricted by the use of physical or logical keys as indicated in Table 2. Authorization is not required for access at level 1.

Table 2 – Authorization requirements - Access levels 2, 3, and 4

Minimum variations of keys	Grade 1	Grade 2	Grade 3	Grade 4
Logical Key	1 000	10 000	100 000	1 000 000
Physical key	300	3 000	15 000	100 000

The requirements specified in Table 2 shall apply to each user.

Depending on the grade, when a CIE uses logical keys to restrict access, or when the CIE has the means to detect incorrect physical keys, means shall be provided to detect and record attempts to gain access by repeated incorrect authorization codes, as specified in Table 3.

When the relevant number of incorrect authorization attempts is detected, the user input device(s) at which the incorrect authorization codes are entered shall be disabled for a minimum of 90 s. Other or all user input devices may also be disabled.

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

Table 3 – Detection of repeated incorrect authorisation codes

	Grade 1	Grade 2	Grade 3	Grade 4
Disable user input device(s)	Op	Op *	M	M
Maximum number of attempts before user input device(s) initially disabled	10	10	10	3
Maximum number of further attempts before user input device(s) disabled	10	10	1	1
Record in event log each time user input device(s) disabled	Op	Op	Op	M
Tamper signal or message	Op	Op *	Op	M
Maximum number of attempts before tamper activated	21	21	21	7
* For Grade 2 at least one these requirements shall be provided.				

8.2.3 Setting procedures

CIE shall provide means for a user, with the appropriate access level, to initiate the setting sequence. During the setting procedure, if an intrusion alarm condition occurs at one or more of the alarm points not allocated to an exit route, the CIE shall as a minimum, generate a local indication and/or notification. The CIE may provide means to set automatically at pre-determined times (time dependent).

When means are provided to set at pre-determined periods, the CIE shall generate at least one indication before setting.

8.2.3.1 Prevention of setting

Means shall be provided to prevent the CIE from initiating and/or completing the setting procedure when one or more of the conditions shown, are present.

Table 4 – Prevention of setting conditions

Prevention of setting conditions	Grade 1	Grade 2	Grade 3	Grade 4
*Detector in active condition	M	M	M	M
Detector range reduction	Op	Op	M	M
Tamper condition	M	M	M	M
Interconnection fault	M	M	M	M
Alternative power source fault	X	X	M	M
Prime power fault	X	X	Op	Op
ATE fault	M	M	M	M
**ATE and WD faults	M	M	M	M
Other IAS component faults	Op	M	M	M
* = Detectors on an agreed exit route may be excluded, only during the exit time, and shall prevent the completion of the setting procedure if still active at the end of the exit period. ** = Faults in all available ATE and WD's which prevent all notification X = One or other function shall be provided				

8.2.3.2 Overriding of prevention of setting

Means may be provided to enable users, as specified in Table 5, to manually override conditions preventing setting. Means may be provided to override conditions preventing setting automatically when setting is time dependent.

Table 5 – Overriding of prevention of setting conditions

Prevention of setting conditions	Grade 1	Grade 2	Grade 3	Grade 4
Detector fault	Level 2	Level 2	Level 2	Level 2
Interconnection fault	Level 2	Level 2	Level 3	Level 3
Alternative power source fault	Level 2	Level 2	Level 2	Level 3
Prime power source fault	Level 2	Level 2	Level 2	Level 2
ATE fault	Level 2	Level 2	Level 3	Level 3
ATE and WD faults	Level 2	Level 2	Level 3	Level 3
Other IAS component faults	Level 2	Level 2	Level 2	Level 3
* NOTE Level 2, if authorised, can be permitted to override for one arming period				

It is permitted at level 2 to override the conditions specified in Table 5 for one set period (EXAMPLE, by inhibiting).

It is permitted at level 3 to override the conditions specified in Table 5 for more than one set period (EXAMPLE, by isolating).

8.2.3.3 Logging the overriding of prevention of setting conditions

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

8.2.3.4 Exit route facility

Provision of an exit route facility is optional.

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

The CIE may provide the means to indicate that the exit procedure has commenced, in accordance with Table 11 and Table 12.

8.2.3.5 Set state

When a CIE is in the set state, means shall be provided (EXAMPLE: an output) to indicate that the CIE is in the set state.

NOTE The intention of the above requirement is to provide a facility to indicate or physically prevent entry into the supervised area when the IAS is set.

8.2.3.6 Failure to set

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

8.2.4 Unsetting procedure

The CIE shall provide means for a user with the appropriate access level, to unset. The CIE may provide means to unset at pre-determined times.

8.2.4.1 Entry route facility

Provision of an entry route facility is optional.

When the CIE provides an entry route facility, means shall be provided to select the defined alarm points to be included in the entry route facility. Means shall be provided to indicate that the entry procedure is running, as specified in Table 11 and Table 12.

8.2.4.2 Entry time

Means shall be provided to limit the time allowed to complete the unsetting procedure to a maximum of 45s, (EXAMPLE: when unsetting is to be initiated from outside the supervised area and completed from inside the supervised area).

8.2.4.3 Alarm condition occurring during the unsetting procedure

When an alarm condition occurs during the unsetting procedure, the alarm condition shall be indicated or notified by an internal warning device only. If the system is not unset within the defined period (45 s maximum) an alarm condition shall be notified immediately.

When remote notification is included in the I&HAS, the alarm condition during the unsetting procedure shall not be remotely notified until the indicator or warning device has operated for a minimum of 30 s.

NOTE The purpose of the above clause, together with EN 50131-1, subclause 8.3.3.3, is to reduce the risk of transmission of alarm notification to the ARC if a detector not included in the entry route is accidentally activated during the unsetting procedure.

8.2.4.4 Entry period exceeded

When the time allowed to complete the unsetting procedure is exceeded, means shall be provided to notify an alarm condition.

8.2.4.5 Indication

Means shall be provided to indicate when the unsetting procedure has been successfully completed and the CIE is unset. The means provided shall not allow the indication to operate for more than 30 s.

8.2.5 Restore function

The CIE shall provide means to restore conditions as defined in Table 6:

Table 6 – Authorisation required to restore conditions

	Grade 1	Grade 2	Grade 3	Grade 4
Intruder	Access level 2	Access level 2	Access level 2	Access level 2
Tamper	Access level 2	Access level 2	Access level 3	Access level 3
Fault	Access level 2	Access level 2	Access level 2	Access level 2
Hold-up	Access level 2	Access level 2	Access level 2	Access level 2

8.2.6 Inhibit function

When an inhibit function is provided, it shall operate in accordance with Table 7 and Table 8. When the CIE is unset, inhibit conditions shall be cancelled.

Inhibit functions shall be applied to individual alarm, tamper, fault or hold up points.

Table 7 – Automatic inhibit

Automatic inhibit	
Intruder Alarm signal or message	OP (after “n” alarm occurrences in a given SET period)
Tamper signal or message	OP (after “n” alarm occurrences in a given SET period)
Fault signal or message	OP (after “n” alarm occurrences in a given SET period)
User interface	OP (EXAMPLE: time window, wrong authorisation code)
Authorisation code	OP (after “m” use, for service personal)
Hold up	Not permitted
NOTE Values of “n” and “m” shall be provided in the manufacturer’s installation documentation.	

Table 8 – Manual inhibit

Manual inhibit					
	Access level	Grade 1	Grade 2	Grade 3	Grade 4
Intruder alarm signal or message	2	Op	Op	Op	Op
	3	Op	Op	Op	Op
Tamper signal or message	2	Op	Op	NP	NP
	3	Op	Op	Op	Op
Fault signal or message	2	Op	Op	NP	NP
	3	Op	Op	Op	Op
Hold up signal or message	2	Op	NP	NP	NP
	3	Op	Op	Op	Op

The CIE may provide means to inhibit other functions within the site-specific programming. Where provided, the manufacturer’s documentation will define how this is achieved. Inhibiting functions shall be indicated according to Table 12 and recorded in the event memory according to Table 15 of EN 50131-1.

8.2.7 Isolate operation

If the CIE includes the means to isolate the operation of one or more functions, access to these means shall be restricted (according the EN 50131-1, subclause 8.3.7) as follows:

- a) access levels 2 or 3 for grades 1 and 2;
- b) access level 3 for grades 3 and 4.

8.2.8 Alarm point soak test mode

In order to provide a tool for the maintenance of the IAS, the CIE may include a soak test function. When this is provided, alarm signals or messages from an alarm point under test shall continue to be recorded in the event log.

The soak attribute can be manually or automatically removed. The manufacturer’s documentation shall specify the criteria for automatic removal of the soak test attribute. Access to initiate and manually remove the soak test function shall be restricted to level 3 in all grades.

Indication of the soak test condition shall be as defined in Table 12.

8.2.9 Other functions

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

Where provided, these additional functions shall not adversely affect the essential requirements of this specification.

8.3 Processing

The CIE shall include the means necessary to process input signals or messages and generate the required output signals or messages and indications (See EN 50131-1, Tables 3, 4 and 5).

8.3.1 Processing of intruder, hold-up, tamper and fault signals or messages

Intruder, hold-up, tamper and fault signals or messages shall be processed and notified as indicated in Table 9.

Table 9 – Processing of intruder, hold-up, tamper alarm and fault signals/messages

*** I&HAS status	Grade 1				Grade 2				Grade 3				Grade 4				
	Inputs Or Outputs	Hold-Up Signal / Message	Intruder Signal / Message	Tamper signal	Fault signal	Hold-Up Signal / message	Intruder Signal / message	Tamper signal	Fault signal	Hold-Up Signal / message	Intruder Signal / message	Tamper signal	Fault signal	Hold-Up Signal / message	Intruder Signal / message	Tamper signal	Fault signal
Set	Indication	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op
	External WD	Op	M	M	M	Op	M	M	M	Op	M	M	M	Op	M	M	Op
	Internal WD	Op	M	M	M	Op	M	M	M	Op	M	M	M	Op	M	M	Op
	ATS Message Type	Hold-Up alarm	Alarm	Alarm or Tamper	Alarm or Fault	Hold Up alarm	Alarm	Alarm or Tamper	Alarm or Fault	**Hold-Up alarm	Alarm	Tamper	Fault	**Hold Up alarm	Alarm	Tamper	Fault
Unset	Indication	Op	*Op	M	M	Op	*Op	M	M	Op	*Op	M	M	Op	*Op	M	M
	External WD	Op				Op				Op				Op			
	Internal WD	Op				Op				Op				Op			
	ATS Message Type	Op as Hold-up	Op as Tamper	Op as Tamper	Op as Fault	Op as Hold-up	Op as Tamper	Op as Tamper	Op as Fault	**Hold-up	Op as Tamper	Op as Tamper	Fault	**Hold-up	Op as Tamper	Op as Tamper	Fault
<p>NOTE The inclusion in Table 9 of requirements relating to warning devices and alarm transmission systems does not imply that I&HAS alarm system 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 9.</p>																	
<p>NOTE Key: M = Mandatory * = On user request Op = Optional Shaded areas = Not permitted</p>																	
<p>NOTE ** information relating to the Zone of the hold-up alarm to be included in the information transmitted to an ARC</p>																	
<p>NOTE *** Signals and/or messages shall be processed according to the status of that part of the I&HAS i.e. set or unset</p>																	
<p>NOTE NOTE This specification permits the independent setting and unsetting of IAS and HAS parts of an I&HAS (8.3.3 refers) it follows that the processing of signals/messages (hold-up, intruder, tamper or fault) from set or unset parts should be processed according to the status (set or unset) of that part of an I&HAS.</p>																	

8.3.1.1 Alarm inputs

Intrusion alarm signals or messages shall be processed individually to generate one or more intruder alarm conditions.

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

8.3.1.2 Priorities

The CIE default priority of signals or message processing shall be described in the manufacturer's documentation. In the event of multiple signals or messages being present simultaneously, all these signals or messages shall be processed and at least one of the highest priority signals or messages shall be notified as indicated in 8.9.5.

8.3.2 Processing of user inputs

When facilities are provided for a user to input signals or messages or commands at the CIE or ACE, processing shall be permitted to verify that the selected functions are authorized according to

- a) the grade,
- b) the access levels as defined in Table 1,
- c) any subset of Table 1 as provided in the manufacturer's documentation.

8.3.3 Monitoring of processing

In CIE with programme controlled serial data processing, means shall be provided to monitor the processing function in accordance with Table 10.

The following requirements shall be provided:

- a) the processing monitoring function (EXAMPLE: watchdog) shall detect a fault with the clock generator within 10 s;
- b) for a grade 4 CIE, an output shall be provided which shall change state when the processing monitoring function activates, this output remaining until manually reset;
- c) for grades 3 & 4, the operation of the processing monitoring function shall attempt to restart the processor and generate a CIE fault signal or message, this event shall be logged and indicated;
- d) when a CIE restarts, as required by c) above, the CIE shall resume operation in its previous operating mode (EXAMPLE: set or unset).

Table 10 – Monitoring of processing

	Grade 1	Grade 2	Grade 3	Grade 4
Processing monitoring function	Op	Op	M	M

8.4 Indication

8.4.1 General

Indications shall be provided and displayed in accordance with the requirements of Table 11 and Table 12.

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

Means may be provided at access level 1 to indicate that information is available to other access levels. (EXAMPLE: audible indicators or flashing visual indicator).

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

8.4.1.1 Alarm, tamper and fault indications

Alarm, tamper and fault indications shall require individual acknowledgement by a user. Following the acknowledgement of an alarm, tamper and fault indication, the indication shall remain at least until the condition is restored.

Acknowledging an indication shall not affect any other indication.

NOTE Acknowledging an indication may be used to silence an audible indicator or change the state of a visible indicator, (EXAMPLE: from flashing to steady).

8.4.1.2 Other conditions

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

Table 11 – Indication (from Table 4 of EN 50131-1)

Conditions to be indicated	Grade 1				Grade 2				Grade 3				Grade 4			
	During setting	Set	During unsetting	Unset	During setting	Set	During unsetting	Unset	During setting	Set	During unsetting	Unset	During setting	Set	During unsetting	Unset
IAS set		Op	Op			Op	Op			M	Op			M	Op	
Alarm condition	M	Op	M	*M		Op	M	*M		Op	M			OP	M	*M
Hold-up alarm	Op	Op	Op	Op	Op	Op	Op	Op	Op	OP	Op	Op	Op	Op	Op	Op
Zone identification	Op	Op	Op	Op	Op	Op	Op	Op	Op		M	Op	Op		Op	Op
Zone isolated	Op	Op	Op	Op	Op	Op	Op	Op	Op		M	Op	Op		M	Op
General fault	M	Op	Op	M	M	Op	M	M	M		M	M	M		M	M
Prime power fault	M	Op	M	M	M	Op	M	M	M		M	M	M		M	M
Alternative power fault	M	Op	Op	M	M	Op	M	M	M		M	M	M		M	M
Zone first to alarm	Op	Op	Op	Op		Op	M	Op			M	M			M	M
Part set	Op	Op	Op	Op	M	Op	M	Op	M		M	Op	M		M	Op
Tamper condition	M	Op	OP	M	M	Op	M	M	M		M	M	M		M	M
ATS fault	M	Op	OP	M	M	Op	M	M	M		M	M	M		M	M
Detector masked	Op	Op	OP	Op	Op	Op	Op	Op	M		M	M	M		M	M

* = Until restored

M = Mandatory

Op = Optional

Shaded area = Not permitted

Table 12 – Additional indication in the CIE or ACE

Conditions to be indicated	Grade 1			Grade 2			Grade 3			Grade 4			
	During setting	Set	During unsetting	During setting	Set	During unsetting	During setting	Set	During unsetting	During setting	Set	During unsetting	Unset
Zone inhibited	Op	Op	Op	M	Op	Op	M	Op	Op	M	Op	Op	Op
Entry/exit indication **	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op
Zone soaked	Op	Op	Op	M	Op	Op	M	Op	Op	M	Op	Op	Op
Monitoring of processing	Op	Op	Op	Op	Op	Op	M	Op	Op	M	Op	Op	M
IAS unset	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	M
Interconnection fault	Op	Op	Op	M	Op	M	M	Op	M	M	Op	M	Op
Power output fault	Op	Op	Op	Op	Op	Op	M	Op	M	M	Op	M	M

Op = Optional M = Mandatory * = Until restored ** = When included Shaded area = Not permitted

NOTE This table is additional to Table 11.

8.4.2 Visual indicators

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

8.4.3 Setting/unsetting indication

Indications shall comply with Table 11 and Table 12, and shall be time limited. Indications of set shall be limited to a maximum of 180 s after the CIE has completed setting. Indications of unset shall be limited to a maximum of 30 s after the CIE has completed unsetting.

8.4.4 Exit/entry route indications

Exit and entry route indications shall be available at access level 1. The CIE may provide other indications. Such indications shall not affect any requirements of this specification.

8.4.5 Priority of indications

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

8.5 Notification outputs

The CIE shall provide one or more outputs to fulfil the requirements described in Table 9. The CIE documentation shall state which option(s) of Table 13 can be fulfilled.

Where the CIE provide outputs for ATE and WDs, means may be provided to delay the operation of WD output/s for a period not exceeding 10 min. Means shall be provided to cancel this delay if a signal or message is received indicating the presence of faults in all available transmissions paths.

Means shall be provided to cancel the operation of the WD outputs providing any previous operation of ATE has resulted in confirmation of successful communications.

Where means are provided by the CIE to operate WDs, these shall operate for a minimum of 90 s and a maximum of 15 min unless other requirements are demanded by local or national regulations.

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

Table 13 – Notification requirements

Means of Notification	Grade 1			Grade 2				Grade 3				Grade 4		
	Op A	Op B	Op C	Op A	Op B	Op C	Op D	Op A	Op B	Op C	Op D	Op A	Op B	Op C
Warning Device	2			2				2				2		
Self-powered WD		1			1				1				1	
First ATS			1	1	1	1	1	1	1	1	1	1	1	1
Second ATS						1				1				1
NOTE 1 The numbers specify the number of devices or systems required.														
NOTE 2 Op refers to the optional means of notification selectable within each grade.														
Op = Optional Shades areas = Not permitted														

8.5.1 Other notification

The CIE may provide other notification outputs. Operation of such outputs shall not affect any requirements of this specification.

8.6 Tamper security (detection/protection)

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

8.6.1 Tamper protection

The CIE and ACE shall be tamper protected according to grade as indicated in Table 14.

Where the CIE is distributed within the housing of other components of the IAS, then the tamper protection of such housings shall comply with Table 14.

Where the CIE is housed in one or more housings, such housings shall be sufficiently robust to prevent undetected access to internal components without visible damage.

Normal access shall be mechanically secure, and require the use of an appropriate tool.

The tests specified in EN 50130-5 shall be applied at the severity levels specified in Table 14.

Table 14 – Tamper protection

	Grade 1		Grade 2		Grade 3		Grade 4	
	Int	Ext	Int	Ext	Int	Ext	Int	Ext
Severity level (IK code)	04	06	04	06	04	06	04	06
Impact energy (Joule)	0,5	1	0,5	1	0,5	1	0,5	1
NOTE Int = inside the supervised premises Ext = outside the supervised premises (indoor or outdoor).								

8.6.2 Tamper detection

Where the CIE is self-contained within its own housing(s), or is distributed within the housing(s) of other components of the IAS, then the tamper detection of such housing(s) shall conform to the requirements of Table 15:

Table 15 -- Tamper detection

Tamper detection	Grade 1	Grade 2	Grade 3	Grade 4
Opening by normal means	M	M	M	M
Removal from mounting*	OP	OP	M	M
Penetration of the housing	OP	OP	OP	M
M = Mandatory OP = Optional *NOTE for Wireless CIE and ACE .				

When opening the CIE or ACE housing/s by normal means, it shall not be possible to introduce a tool, as specified in Table 16 and EN 60529, without operating the tamper detection.

In grades 1 and 2 this requirement does not include indicators or operating controls (EXAMPLE: push-buttons, keypads, LCD or graphic screens); in grades 3 and 4 such indicators and operating controls are included.

Table 16– Tool dimension for tamper detection

	Grade 1	Grade 2	Grade 3	Grade 4
Steel rod diameter, mm (± 0,05 mm)	2,5	2,5	1	1

8.6.2.1 Removal from mounting

CIE and ACE using wireless interconnections shall include means to detect removal from the mounting surface as specified in Table 15 and Table 17.

Table 17– Removal from mounting

	Grade 1	Grade 2	Grade 3	Grade 4
Maximum distance before tamper detection	25 mm	10 mm	5 mm	5 mm

8.6.2.2 Penetration of the housing

CIE and ACE shall include means to detect penetration of the housing as specified in Table 15, when a hole of 4 mm is made in the housing.

8.7 Fault

Dependent on the grade, CIE shall include means to recognize the fault conditions as specified in Table 18.

Table 18 – Recognition of fault conditions

Faults	Grade 1	Grade 2	Grade 3	Grade 4
Prime power fault	M	M	M	M
Alternative power fault	M	M	M	M
Battery change required (*)	M	M	M	M
Power output fault (**)	Op	Op	M	M
ATS fault	M	M	M	M
CIE fault	Op	Op	M	M
Interconnections	M	M	M	M
Warning Device	M	M	M	M
Other components	M	M	M	M
Detector fault	M	M	M	M
ATE	M	M	M	M
General fault	M	M	M	M
Monitoring of processing	Op	Op	M	M
EPS	M	M	M	M
(*) = applies to primary cells only (type "C"PS)		M = Mandatory		
(**) = as in 50131-6 sec 4.2.1		Op = Optional		

8.8 Interconnections

8.8.1 Providing interconnection facility

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

Specific (or dedicated) wired interconnections are dedicated links which can be direct connections carrying voltage signals or dedicated data bus connections carrying messages. A CIE may use direct and/or data bus connections.

8.8.2 Monitoring of interconnection function

The CIE shall include means to confirm that the interconnection function is operating normally.

The CIE shall expect to receive confirmation, from the interconnection function, that the interconnections are operating normally within the times specified in the Table 19.

Table 19 – Interconnection confirmation

	Grade 1 minutes	Grade 2 minutes	Grade 3 seconds	Grade 4 seconds
Interconnection confirmation	240	120	100	10

When it is established that interconnection confirmation could not be verified due to a fault condition, a fault signal or message shall be generated in all grades:

When the interconnection confirmation could not be verified due to a condition other than a fault, a tamper or fault signal or message shall be generated as follows:

- a) grade 1 & 2 fault or tamper;
- b) grade 3 & 4 tamper.

8.8.3 Processing signals from interconnections

Tamper or fault signals or messages, received from the interconnection function, shall be processed in accordance with Table 9.

8.9 Timing

Signals and messages shall be processed as specified below.

NOTE NOTE 1 Immunity to accidental recognition of an alarm signal due to electrical interference (e.g. E.M.I.) is addressed in EN 50130-4.

NOTE NOTE 2 Annex A describes different type of interconnection.

NOTE NOTE 3 Annex C includes a summary of the timing requirements.

8.9.1 Intruder signals or messages.

Intruder alarm signals with an active period exceeding 400 ms shall be processed as intruder alarm conditions. Shorter duration intruder alarm signals may be processed.

Intruder alarm messages shall be processed as intruder alarm conditions.

8.9.2 Hold-up signals or messages

Hold-up alarm signals with an active period exceeding 400 ms shall be processed as hold-up alarm conditions. Shorter duration hold-up alarm signals may be processed.

Hold-up alarm messages shall be processed as hold-up alarm conditions.

8.9.3 Tamper signals or messages

Tamper alarm signals with an active period exceeding 400 ms shall be processed as tamper alarm conditions. Shorter duration tamper alarm signals may be processed.

Tamper alarm messages shall be processed as tamper alarm conditions.

8.9.4 Fault signals or messages

Fault signals with an active period exceeding 10 s shall be processed as fault conditions. Shorter duration fault signals may be processed.

Fault messages shall be processed as fault conditions.

8.9.5 Processing timing

Intruder, tamper, hold-up and fault signals and/or messages shall be processed and notification shall be initiated within 10 s.

8.10 Event recording

Event recording shall be in accordance with EN 50131-1.

Each new mandatory event (as defined in EN 50131-1) shall be recorded within 10 s of the occurrence of the event.

The CIE shall include means to record the events specified in EN 50131-1 or to permit events to be recorded at an ARC or other remote location.

Recording of the mandatory events shall not be affected, neither overwritten by the recording of any non-mandatory event (EXAMPLE: separate event logs).

8.10.1 Alteration or deletion

The CIE shall not include facilities to alter or delete the contents of the event log, except as permitted in 8.10.2.

8.10.2 Capacity

According to the grade, the minimum capacity of the CIE event log shall be as specified in EN 50131-1. When the capacity of the event log is reached, the oldest event recorded may be discarded.

NOTE The event log may be cyclic, (EXAMPLE: a "first in – first out" file, where the newest event overwrites the oldest one) or permanent (EXAMPLE: a print out).

8.10.3 Time and date

In grades 2, 3 and 4 CIE, each event shall be stored together with the time and date that the event occurred. This information shall be accurate to within 10 min per annum.

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

8.10.4 Retention following power failure

The event log shall retain its stored data for a minimum of 30 days when both the PPS and the APS have failed.

8.10.5 Number of events from single source

Means shall be provided to avoid multiple events generated from a single source filling the event log.

The number of repeated events, excluding user actions or soak test events from the same source during any set or unset period shall be limited to three.

8.10.6 Permanent record facility

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

When a permanent record is made, it shall include all mandatory stored events, including time and date.

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

8.10.7 Event recording at the ARC or other remote location

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

When events cannot be transferred, in grades 1 and 2, a fault condition shall be generated., In grades 3 and 4, events that have failed to be transmitted shall be stored temporarily in the CIE. The requirements for this temporary memory shall be in accordance with the requirements of EN 50131-1, Table 14.

8.11 Power supply

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

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

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

NOTE The system designer (installer) will need to calculate the total stand-by period required for the IAS, according to the grade of the IAS, as indicated in EN 50131-1.

9 Electrical safety

The CIE shall comply with the requirements of EN 60950 or EN 60065.

10 Product documentation

10.1 Installation and maintenance

The following information shall be provided:

- a) installation, commissioning and maintenance requirements including terminal identifications, in accordance with this Technical Specification;
- b) security grade for which CIE and ACE are suitable;
- c) type of PS, with the related voltage rating and frequency requirements of the PPS source and the output voltage and maximum current rating;
- d) type of SD, if provided, and maximum capacity (V, Ah), and maximum recharge time;
- e) technical specification (EXAMPLE: dimensions, weight, construction material);
- f) values of “n” and “m”, as specified in Table 7;
- g) the minimum number of variations of logical keys and/or physical keys for each user;
- h) the number and details of disallowed codes;
- i) the method used to determine the number of combinations of logical keys and/or physical keys;
- j) programmable functions provided;
- k) operating temperature range;
- l) where there are serviceable parts (EXAMPLE: fuses) their type and value shall be given;
- m) environmental class;
- n) name or mark of certification body (if any);
- o) standard to which component claims compliance;
- p) the current consumption of the CIE and each type of ACE device, with and without an alarm condition;
- q) the maximum number of each type of ACE device;
- r) the maximum current rating of each output.

10.2 Operating instructions

The following information shall be provided.

- a) operating instructions;
- b) security grade to which the CIE and ACE comply;
- c) values of “n” and “m”, as specified in Table 7;
- d) the minimum number of variations of logical keys and/or physical keys for each user;
- e) the number and details of disallowed codes;
- f) user programmable functions provided;
- g) where there are user serviceable parts (EXAMPLE: fuses) their type and value shall be given;
- h) environmental class.

11 Marking and labelling

The CIE and ACE shall be marked with the following:

- a) name of manufacturer or supplier;
- b) type or model name or number;
- c) date of manufacture or batch number or serial number;
- d) security grade;
- e) environmental class;
- f) nominal voltage, current and frequency of the PPS.

These markings shall be legible, durable and unambiguous. Where space for marking a CIE or ACE is limited, codes may be used providing these are described in the associated documentation. Where insufficient space is available for codes, the CIE or ACE shall include means of identification which allows cross reference to documentation providing the required information.

12 Tests

12.1 Test conditions

12.1.1 Laboratory conditions and tolerance

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

- temperature: 15 °C to 35 °C
- relative humidity: 25 % to 75 %
- air pressure: 86 kPa to 106 kPa

12.1.2 Mounting

The CIE shall be mounted in accordance with the manufacturer's installation instructions.

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

All input signals (EXAMPLE: directly wired zone inputs or bus line) shall be correctly terminated according to the manufacturer's instructions.

12.1.3 CIE test configuration

The manufacturer shall provide a CIE, configured as required in this specification.

The CIE shall include at least one type of each ACE for which the manufacturer requires the approval tests.

The balance of the ACE configuration may be simulated.

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

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

The alarm points being monitored for the purposes of the test(s) shall be programmed in accordance with the manufacturer's instructions.

- a) Site specific parameters: The manufacturer shall state the programming parameters and adjustments that may affect the ability of the CIE to meet the requirements of the specification.
- b) Hardware: The manufacturer shall provide equipment to the test house as defined below:
 - Where the maximum configuration is up to 100 alarm points, a CIE shall be connected with the maximum number of alarm points.
 - Where the maximum configuration is greater than 100 alarm points, a CIE shall be connected with 100 alarm points plus 10 % of the balance of the maximum (EXAMPLE: CIE with a maximum of 500 alarm points will have a nominal test configuration of $100 + \left(\frac{500 - 100}{10} \right) = 140$ alarm points). The maximum number of alarm points shall be 200.
- c) The event log may be pre-filled by the manufacturer before the test.

12.1.4 Power supply

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

12.1.5 Documentation

12.1.5.1 Product

The product documentation (as required in Clause 10) shall be provided with the CIE.

12.1.5.2 Simulator test device

If additional equipment (EXAMPLE: a simulator or a programmable device) is supplied by the manufacturer (as in 12.1.3) connection drawings, operational description and instructions for use shall be supplied.

12.2 Functional tests

All functional tests described in 12.4 shall be carried out.

The pass-fail criteria are given in each test.

NOTE 1 Shock and impact tests are covered by tamper protection requirements.

NOTE 2 ESD and EMI tests are covered by the related EMC Directives.

12.3 Reduced functional test

On completion of specified tests, (EXAMPLE: environmental tests), it may not be possible or desirable to carry out a full functional test; in these cases a reduced functional test shall be carried out in accordance with Table 20.

Table 20 – Reduced functional test

Step	Test condition (c)	Action (d)	Measurement (e)	Pass/fail criteria (f)
1	CIE unset, Absence of “intruder, tamper, fault signals and messages”, No indication active	Apply an alarm signal or message as specified in 8.8 and 8.9.	Check indications	Indications shall be according to the Grade (as shown in Table 11 and Table 12)
2	As above plus: one alarm input, <i>not allocated as an “entry route”</i>	Attempt to set the system	Record whether the system sets	The system should be prevented from setting
3	As in 1) above	Set the system	Record indications	Indications shall be according to the Grade (as shown in Table 11 and Table 12)
4	CIE set	Apply an alarm signal or message as specified in 8.8 and 8.9.	Record the status of the output for external warning devices	The output for the external warning device shall be activated in accordance with 8.3.1
5	CIE in “set” and in “alarm” conditions	Unset the CIE	Record whether the system unsets and the status of the output for the external warning devices and ATEs and check the event log (Grades 2, 3 and 4)	CIE unset, Indications and notifications shall be according to the Grade (as shown in Table 11 Table 12 and Table 13). Correct time and events sequences recorded

12.4 Functional tests

12.4.1 Processing intruder alarm signals or messages

(requirement: 8.1.1 – 8.2.5 – 8.3.1 -8.3.1.2 - 8.9.1 – 8.9.5– 8.10 – 8.10.5)

a) Object of the test

To demonstrate the ability of the CIE to:

- i. receive and process an intruder signal or message, within the processing timing requirements of this specification, when the CIE is in the set, and the unset conditions;
- ii. provide indication(s) and notification(s);
- iii. correctly record the event(s) in the event log;
- iv. restore in accordance with 8.2.5.

b) Principle

The test consists of applying an intrusion signal/message as specified in 8.9 to an intruder input, and monitoring that the input has been processed within the required time period, and that the correct indication and notification(s) occur, see Table 21.

Table 21 – Functional tests

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	<p><i>GENERAL CONDITION</i></p> <p><i>The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.</i></p> <p><i>When multiple methods to set and to unset the CIE are provided, then the test shall be carried out for each method</i></p>		<p>GENERAL MEASUREMENT</p> <p>Record the condition of the indication and notification outputs of the CIE, and any associated user input devices (EXAMPLE remote keypads).</p> <p>Time when signal applied.</p> <p>Time when notification occurs.</p> <p>Record the event log</p>	<p><i>GENERAL CRITERIA</i></p> <p>Processing shall be in accordance with Table 9 and 8.3.1</p> <p>The indications and notifications shall be in accordance with Table 11 Table 12 and Table 13</p>
1	C.I.E in "Set mode"	Apply Intruder signal as specified in 8.8 and 8.9.1	General measurement + Record the identity of the alarm point being activated.	General criteria + As defined in 8.9.5, notification shall occur within 10 s of the test Intruder signal or message being applied. The logging shall be in accordance with 8.10
2	CIE "in set mode" (with alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4
3	CIE "in unset mode"	Restore (EXAMPLE: by entering a correct PIN number into the keypad)	General measurement	In accordance with 8.2.5
4	CIE in "set mode" NOTE To verify that multiple signals or messages applied at the same alarm point, are not recorded more than 3 times in the event log.	Apply the same intruder signal as specified in 8.8 and 8.9.1 four times Afterwards repeat step 3	General measurement	Not more than 3 intruder alarms from the same source shall be recorded as specified in 8.10.5
5	CIE "in unset mode"	Apply Intruder signal as specified in 8.8 and 8.9.1	General measurement	General criteria
6	CIE in "unset mode" NOTE To verify that intruder signals or messages are not recorded in the event log.	Apply the same intruder signal as specified in 8.8 and 8.9.1 four times Afterwards repeat step 3	General measurement	General criteria

7	CIE in "set mode". Note: to verify that if multiple signals or messages are applied, at least one is processed correctly	Apply intruder signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE, or 5 (whichever is the greater) within 1 s	General measurement	At least one intruder signal or message shall be processed in accordance with 8.3.1.2 and 8.9.5
8	CIE "in set mode" (with more than one alarm condition)	Unset the C.I.E	General measurement	General criteria Indications shall comply with 8.4
9	CIE "in unset mode"	Restore all the conditions	General measurement	In accordance with 8.2.5

12.4.2 Processing of hold-up signals or messages

a) Object of the test

To demonstrate the ability of the CIE to comply with 8.1.2, 8.2.3.1, 8.2.5 - 8.3.1, 8.4, 8.5, 8.9.2, 8.9.5, 8.10, 8.10.5 and to:

- i. receive and process a hold-up signal or message, within the processing timing requirements of this specification, when the CIE is in the set, and the unset conditions;
- ii. provide indication(s) and notification(s);
- iii. correctly record the event(s) in the event log;
- iv. restore in accordance with 8.2.5.

b) Principle

The test consists of applying a hold-up signal as specified in 8.9 or a hold-up message compatible to the CIE to a hold-up input when the system is in a variety of conditions shown in Table 22 below. The system shall be monitored to ensure that the input has been processed within the required time period, and that the correct indication(s), notification(s) and event recording occur.

Table 22 – Tests of the processing of hold-up signal or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	<p><i>GENERAL CONDITION</i></p> <p><i>The CIE is in the condition described in the steps below, with all inputs and outputs in normal condition</i></p> <p><i>When multiple methods to set and to unset the CIE are provided, then the test shall be carried out for each method</i></p>		<p>GENERAL MEASUREMENT</p> <p>Record the condition of the indication and notification outputs of the CIE, and any associated user input devices (EXAMPLE remote keypads)</p> <p>Time when signal applied</p> <p>Time when notification occurs</p> <p>Record the event log</p>	<p><i>GENERAL CRITERIA</i></p> <p>Processing shall be in accordance with Table 9 and 8.3.1</p> <p>The indications and notifications shall be in accordance with Table 11 Table 12 and Table 13</p>

1	C.I.E in "Set mode"	Apply hold-up signal as specified in 8.8 and 8.9.2	General measurement + Record the identity of the alarm point being activated.	General criteria + As defined in 8.9.5, notification shall occur within 10 s of the test hold-up signal or message being applied The logging shall be in accordance with 8.10
2	CIE "in set mode" (with alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4
3	CIE "in unset mode"	Restore	General measurement	In accordance with 8.2.5
4	CIE in "set mode" Note: to verify that multiple signals or messages applied at the same alarm point, are not recorded more than 3 times in the event log.	Apply the same hold-up signal or message as specified in 8.8 and 8.9.2 four times Afterwards repeat step 3	General measurement	Not more than 3 hold-up alarms from the same source shall be recorded as specified in 8.10.5
5	CIE "in unset mode"	Apply hold-up signal as specified in 8.8 and 8.9.2	General measurement	General criteria
6	CIE in "unset mode" NOTE To verify that intruder signals or messages are not recorded in the event log.	Apply the same hold-up signal as specified in 8.8 and 8.9.2 four times Afterwards repeat step 3	General measurement	General criteria
7	CIE in "set mode". NOTE To verify that if multiple signals or messages are applied, at least one is processed correctly.	Apply hold-up signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE, or 5 (whichever is the greater) within 1 s.	General measurement	At least one hold-up signal or message shall be processed in accordance with 8.3.1.2 and 8.9.5
8	CIE "in set mode" (with more than one alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4
9	CIE "in unset mode"	Restore all the conditions	General measurement	In accordance with 8.2.5

12.4.3 Processing of tamper signals or messages

a) Object of the test

To demonstrate the ability of the CIE to comply with 8.1.3, 8.3.1, 8.4.1, 8.5, 8.6, 8.9.3, 8.9.5, 8.10 and to:

- i. receive and process a tamper signal or message, within the processing timing requirements of this specification, when the CIE is in the set, and the unset conditions;
- ii. provide indication(s) and notification(s);
- iii. correctly record the event(s) in the event log;
- iv. restore in accordance with 8.2.5.

b) Principle

The test consists of applying a tamper signal as specified in 8.8 and 8.9 or a tamper message compatible with the CIE, to a tamper input when the system is in a variety of conditions shown in Table 23 below. The system shall be monitored to ensure that the input has been processed within the required time period, and that the correct indication(s), notification(s) and event recording occur.

Table 23 – Tests of the processing of tamper signal or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	<p><i>GENERAL CONDITION</i></p> <p><i>The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.</i></p> <p><i>When multiple methods to set and to unset the CIE are provided, then the test shall be carried out for each method</i></p>		<p>GENERAL MEASUREMENT</p> <p>Record the condition of the indication and notification outputs of the CIE, and any associated user input devices (EXAMPLE remote keypads).</p> <p>Time when signal applied.</p> <p>Time when notification occurs.</p> <p>Record the event log</p>	<p><i>GENERAL CRITERIA</i></p> <p>Processing shall be in accordance with Table 9 and 8.3.1.</p> <p>The indications and notifications shall be in accordance with Table 11 Table 12 and Table 13.</p>
1	C.I.E in "Set mode"	Apply tamper signal as specified in 8.8 and 8.9.3	General measurement + record the identity of the alarm point being activated.	General criteria + As defined in 8.9.5, notification shall occur within 10 s of the test tamper signal or message being applied. The logging shall be in accordance with 8.10
2	CIE "in set mode" (with intruder alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4
3	CIE "in unset mode"	Restore	General measurement	In accordance with 8.2.5
4	CIE in "set mode" Note: to verify that multiple signals or messages applied at the same alarm point, are not recorded more than 3 times in the event log.	Apply the same tamper signal as specified in 8.8 and 8.9.3 four times Afterwards repeat step 3	General measurement	Not more than 3 tamper alarms from the same source shall be recorded as specified in 8.10.5
5	CIE "in unset mode"	Apply tamper signal as specified in 8.8 and 8.9.3	General measurement	General criteria
6	CIE in "unset mode" Note: to verify that intruder signals or messages are not recorded in the event log.	Apply the same tamper signal as specified in 8.8 and 8.9.3 four times Afterwards repeat step 3	General measurement	General criteria

7	CIE in "set mode". Note: to verify that if multiple tamper signals or messages are applied, at least one is processed correctly.	Apply tamper signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE, or 5 (whichever is the greater) within 1 s.	General measurement	At least one tamper signal or message shall be processed in accordance with 8.3.1.2 and 8.9.5
8	CIE "in set mode" (with more than one tamper alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4.1.1 and Table 11
9	CIE "in unset mode"	Restore all the conditions	General measurement	In accordance with 8.2.5

12.4.4 Tamper protection (normal access)

a) Object of the test

To demonstrate that normal access to the internal components of the CIE and ACE comply with 8.6.1 (without visible damage being caused to the CIE and ACE enclosure) requires an appropriate tool.

b) Principle

The test consists of verifying that a tool is required for normal access.

c) Test conditions

The CIE and/or ACE enclosure shall be mounted and secured closed, according the manufacturer's instructions.

d) Test procedure

Tests shall be carried out, first trying to open the enclosure(s) with the tool(s) specified by the manufacturer and then by opening the enclosure(s) without tools.

e) Measurement

Record any visible damage and the status of the enclosure(s), open or closed.

f) Pass/fail criteria

- i. The use of the appropriate tool shall allow access to the internal components.
- ii. Access to the internal components of the CIE and ACE without the defined tool shall not be achieved without visible damage.

12.4.5 Tamper protection (impact)

a) Object of the test

To demonstrate the ability of the CIE and ACE to comply with 8.6.1 to prevent access to its internal components without visible damage.

b) Principle

The principle consists of applying the tests specified by EN 50130-5 (for impact test only), at the severity levels defined in Table 14.

c) Test conditions

The CIE and ACE enclosure(s) shall be mounted and secured closed according the manufacturer's instructions and the device shall not be powered.

Test conditions shall be as specified in EN 50130-5.

d) Test procedure

The test procedure shall be as specified in EN 50130-5.

The impacts shall be applied on the visible faces of the enclosure(s) and (depending on the grade) not on the indicators and operating controls (such as push-button, keypads, LCD (Liquid Crystal Displays) or graphic screens).

e) Measurement

Record any visible damage and the status of housing, open or closed.

f) Pass/fail criteria

- i. Access to the internal components shall not be achieved without visible damage.
- ii. Following the application of the test, if there is no visible damage, the device shall be subjected to the reduced functional test.

12.4.6 Tamper detection

a) Object of the test

To demonstrate the ability of the CIE and ACE to comply with 8.1.3, 8.6.2, 8.9.3, 8.9.5, 8.10 and to generate a tamper signal or message, according to the security grade, when the enclosure is opened by normal means. The tests shall be performed with the CIE in each of the operating modes to ensure that tamper detection satisfies all relevant requirements.

b) Principle

The test consists of verifying that a tamper signal or message is generated before it is possible to insert the test rod when the enclosure is being opened.

c) Test conditions

The device shall be mounted according to the manufacturer's specifications, the tests shall be performed with the CIE set and unset.

d) Test procedure

Using the appropriate tool as specified by the manufacturer, open the enclosure.

Whilst opening, attempt to introduce a test rod (as specified in EN 60529) into the housing.

e) Measurement

Record the generation of the tamper signal or message.

f) Pass/fail criteria

When opening the enclosure using the tool specified by the manufacturer, according to the grade, it shall not be possible to introduce the test rod (with the dimensions specified in Table 16) without generating a tamper signal or message.

12.4.7 Removal from mounting**a) Object of the test**

To demonstrate the ability of wire-free CIE or ACE to comply with 8.6.2.1 to generate a tamper signal, according to the security grade, when the device is removed from its mounting.

b) Principle

The test consists of verifying that a tamper signal is generated when the device is removed from its mounting.

c) Test conditions

The device shall be mounted as recommended by the manufacturer in the installation instructions. The tests shall be performed with the CIE in set and unset modes.

d) Test procedure

Gradually remove the housing from its mounting whilst monitoring the generation of the tamper signal or message.

e) Measurement

Record the generation of the tamper signal or message.

f) Pass/fail criteria

The tamper signal or message shall be generated when the enclosure is moved from its mounting surface in accordance with 8.6.2.1.

12.4.8 Penetration**a) Object of the test**

To demonstrate the ability of the CIE or ACE to comply with 8.6.2.2 to generate a tamper signal or message, according to the security grade, when the enclosure is penetrated.

b) Principle

The test consists of verifying that a tamper signal or message is generated when the enclosure is penetrated.

c) Test conditions

The device shall be mounted as recommended by the manufacturer in the installation instruction on a flat surface (EXAMPLE: a test bench or a rack). The tests shall be performed with the CIE in set and unset modes. When the detection is made using a light sensitive device then the test shall be carried out both in high (500 lux +/- 5 %) and in low (5 lux +/- 5 %) light conditions.

d) Test procedure

Create a hole by penetrating completely through the material of the enclosure into the internal free space, whilst monitoring for the generation of a tamper signal or message.

e) Measurement

Record the generation of a tamper signal or message.

f) Pass/fail criteria

The tamper signal or message shall be generated when the penetration creates a hole with a minimum of 4 mm diameter in the enclosure.

12.4.9 Process monitoring

a) Object of the test

To demonstrate the ability of the CIE with programme controlled serial data processing to comply with 8.3.3 to detect and react to faults with the clock generator.

b) Principle

The test consists of introducing a fault in the clock and monitoring that the correct indication(s) and notification(s) occur, see Table 24.

Table 24 – Test of the process monitoring

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	The CIE shall be in the unset mode, with all inputs and outputs in normal condition.	Introduce a short circuit across the clock generation circuit.	Record the status of process monitoring output.	The watchdog output shall change state within 10 s In Grade 4 the output shall change status within 10 s.
2		Remove short circuit and apply the reduced functional test.	Record the status of the CIE, the event log and the indications.	In Grades 3 and 4 the processor shall restart and the CIE shall resume in its previous operating mode. The reduced functional test shall be completed successfully. A CIE fault shall be indicated. A CIE fault shall be recorded in the event log.
3	Repeat steps 1 & 2 as above for "set mode".	Repeat as above	As above	As above

12.4.10 Processing of fault signals or messages

a) Object of the test

To demonstrate the ability of the CIE to comply with 8.1.4, 8.2.5, 8.3.1, 8.4.1, 8.5, 8.7, 8.9.4, and 8.10 to receive, process, log and notify a fault signal or message, within the requirements of this specification. The tests shall be performed with the CIE in set and unset modes to ensure that detection of faults satisfies all relevant requirements.

b) Principle

To demonstrate the ability of the CIE to:

- i. receive and process a fault signal or message, within the processing timing requirements of this specification, when the CIE is in the set, and the unset conditions;
- ii. provide indication(s) and notification(s);
- iii. correctly record the event(s) in the event log;
- iv. restore in accordance with 8.2.5.

The test consists of applying fault conditions as specified in 8.7.

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

Table 25 – Test of processing of fault signals or messages

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	<p><i>GENERAL CONDITION</i></p> <p><i>The CIE is in the condition described in the steps below with all inputs and outputs in normal condition.</i></p> <p><i>When multiple methods to set and to unset the CIE are provided, then the test shall be carried out for each method</i></p>		<p>GENERAL MEASUREMENT</p> <p>Record the condition of the indication and notification outputs of the CIE, and any associated user input devices (EXAMPLE remote keypads).</p> <p>Time when signal applied.</p> <p>Time when notification occurs.</p> <p>Record the event log</p>	<p><i>GENERAL CRITERIA</i></p> <p>Processing shall be in accordance with Table 9 and 8.3.1.</p> <p>The indications and notifications shall be in accordance with Table 11 Table 12 and Table 13.</p>
1	C.I.E in "Set mode"	Apply fault signal as specified in 8.8 and 8.9.4	General measurement + Record the identity of the alarm point being activated.	General criteria + Notification shall occur within 10 s of the test fault signal or message being applied as defined in 8.9.5 The logging shall be in accordance with 8.10
2	CIE "in set mode" (with alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4

3	CIE "in unset mode"	Restore	General measurement	In accordance with sub Clause 8.2.5
4	CIE in "set mode" Note: to verify that multiple signals or messages applied at the same alarm point, are not recorded more than 3 times in the event log.	Apply the same fault signal as specified in 8.8 and 8.9.4 four times Afterwards repeat step 3	General measurement	Not more than 3 fault alarms from the same source shall be recorded as specified in 8.10.5
5	CIE "in unset mode"	Apply fault signal as specified in 8.8 and 8.9.4	General measurement	General criteria
6	CIE in "unset mode" Note: to verify that repetitive fault signals or messages are not recorded in the event log.	Apply the same fault signal as specified in 8.8 and 8.9.4 four times Afterwards repeat step 3	General measurement	General criteria
7	CIE in "set mode". Note: to verify that if multiple signals or messages are applied, at least one is processed correctly.	Apply fault signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE, or 5 (whichever is the greater) within 1 s.	General measurement	At least one fault signal or message shall be processed in accordance with 8.3.1.2 and 8.9.5
8	CIE "in set mode" (with more than one alarm condition)	Unset the C.I.E.	General measurement	General criteria Indications shall comply with 8.4
9	CIE "in unset mode"	Restore all the conditions	General measurement	In accordance with 8.2.5
10	CIE in "set mode"	Apply intruder, hold-up, tamper or fault signals or messages equivalent to 5 % of the maximum alarm point capacity of the CIE, or 5 (whichever is the greater) within 1 s.	General measurement + Record the identity of the intruder, hold up, tamper and fault being activated.	General criteria + All the conditions shall be correctly identified and logged in the event log at the correct time.

12.4.11 Processing of optional functions (non specified in EN 50131-1)

a) Object of the test

To demonstrate the ability of the CIE to comply with 8.1.7, 8.9 and 8.10 which includes optional functions to receive and process an intruder, hold-up, tamper or fault signals or messages within the processing timing requirements of this specification, when the CIE is in the set, and the unset conditions and one or more optional signals are present.

b) Principle

The test consists of applying a mandatory signal or message, while an optional signal or message is applied to another input of the CIE and monitoring that the mandatory signal or message has been processed within the required time period, and that the correct indication and notification(s) occur.

Table 26 – Test of processing of optional functions (non specified in EN 50131-1)

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	C.I.E in “unset mode”	Apply an optional signal or message to the input(s) of the CIE Within 500 ms after applying the optional signal or message apply a mandatory signal or message to an input of the CIE	Record: - the status of the notification outputs - the time period between the input of the mandatory signal or message and the initiation of the mandatory notification	Notification, arising from the input of the mandatory signals or messages, shall be initiated within 10 s
2	C.I.E in “Set mode”	Repeat as above	As above	As above

12.5 Access level**12.5.1 Access to the functions and controls****a) Object of the test**

To demonstrate the ability of the CIE to comply with 8.2.1, 8.1.6, 8.2.3.2, 8.2.5, 8.2.7, 8.2.8, 8.3.2 and 8.10 to provide up to four levels of access and verify the relevant access to the functions and controls.

b) Principle

The test consists of attempting to use the functions and the controls shown in Table 1, operating the CIE at each access level and verifying that access is granted for permitted functions, and is denied for non-permitted functions.

Table 27 – Test of the access to the functions and controls

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	The CIE and any necessary ACE shall be mounted according to the manufacturer's specifications.	At access level 1 attempt to operate all the functions and controls listed in Table 1, Table 5, Table 6 Table 8 and 8.2.7 and 8.2.8	Record whether access is permitted.	Access is in accordance with Table 1, Table 5, Table 6 Table 8 and 8.2.7 and 8.2.8
2	As above	Repeat as above for access level 2	As above	As above
3	As above	Repeat as above for access level 3	As above	As above
4	As above	Repeat as above for access level 4	As above	As above

12.6 Authorization requirements

(Requirement: 8.2.2) Authorisation

12.6.1 Logical key tests

a) Object of the test

To verify the logical key variations, as specified in Table 2, are provided by the CIE and any associated ACE.

To verify the manufacturer's documentation complies with the requirements of 10.1.

b) Principle

Verify that the range of combinations of logical keys is provided.

Confirm that invalid codes are not accepted.

c) Test conditions

For the test purpose, the manufacturer shall provide to the test-house the following information (refer to informative Annex B):

- i. the number of disallowed codes;
- ii. the method used to determine the number of combinations;
- iii. for each user, the minimum number of variations of logical key shall be indicated.

d) Test procedure

- i. Create samples of valid codes as described in the CIE documentation. The number of valid codes to be created shall be: 10 for Grade 1; 20 for Grade 2; 50 for Grade 3; 100 for Grade 4.
- ii. Attempt to create an invalid code.
- iii. Verify the validity of the manufacturers calculations.

e) Measurement

- Record the valid codes.
- Record the invalid code .

f) Pass/fail criteria

- i. All valid codes created in d) i) above shall be accepted according to grade.
- ii. Invalid codes shall not be accepted.
- iii. Calculations shall be shown to be in accordance with code differs shown in Table 2.

12.6.2 Physical key tests

a) Object of the test

To verify the physical key variations, as specified in Table 2, are provided by the CIE and any associated ACE.

To verify the manufacturer's documentation complies with the requirements of Clause 10.

b) Principle

Verify the range of combinations of physical keys are provided.

To confirm that invalid physical keys are not accepted.

c) Test conditions

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

- i. the number of key variations;
- ii. the method used to determine the number of key variations.

d) Test procedure

- i. Attempt to change the state of the CIE using a valid key.
- ii. Attempt to change the state of the CIE using a non valid key.
- iii. Examine the manufacturer's information regarding key construction and calculations.

e) Measurement

- i. Verify that the manufacturer's information and calculations are valid.
- ii. Note the state of the CIE before and after use of valid key.
- iii. Note the state of the CIE before and after attempted use of non-valid key.
- iv. Record details of the invalid keys.

f) Pass/fail criteria

- i. The valid key changes the state of the CIE.
- ii. The non-valid key does not change the state of the CIE.
- iii. The manufacturer's supplied information and calculations confirm that the number of differs complies with Table 2.

12.6.3 Incorrect authorization codes**a) Object of the test**

Verify that the detection and notification of attempted entry of incorrect authorization codes complies with 8.2.2 and Table 3.

b) Principle

The test consists of entering a series of invalid authoriation codes and establishing that when the number of invalid codes have been entered as specified in Table 3, the user input is disabled, and/or a tamper signal or message is generated and recorded in the event log as specified Table 3.

Table 28 – Test for disabling user input during incorrect authorization codes

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
If the CIE has the facility to disable user input carry out this series of tests				
	GENERAL: The CIE shall be configured with its inputs and outputs in their normal condition, allowing the CIE to be set and alarms to be generated from at least 1 alarm point.	GENERAL: The steps 2,4,5,6, and 7 shall be repeated in the "UNSET" mode of the CIE		
1	CIE unset	Enter a valid authorisation code and attempt to set CIE	Record status of CIE	CIE set
2	CIE set	Enter a series of invalid codes according to Table 3 to attempt to initially disable the user input device.	Record status of CIE, disabling of user input, tamper conditions and event log	CIE should not change state, the user input shall be disabled, the generation of tamper conditions and event log shall be in accordance with Table 3
3	CIE set	During the "disabling time" apply an alarm signal or message	Record whether the alarm condition is processed	The alarm generated during the disable period shall be processed in accordance with Table 9
4	Cie set	During the "disabling time" try to enter a correct code	Record whether user input is available	The CIE shall not change state The user input shall be disabled
5	CIE set	When disabling time has expired, enter another series of invalid codes according to Table 3	Record status of CIE, disabling of user input, tamper conditions and event log	The CIE shall not change state, and shall be in accordance with Table 3
6	CIE Set	During the "disabling time" try to enter a correct code	Record whether user input is available	The CIE shall not change state The user input shall be disabled in accordance with Table 3
7	CIE Set	When disabling time has expired enter a valid user code and attempt to change state of the CIE	Record status of the CIE	The CIE shall change state

Table 29 – Test for generation of tamper during incorrect authorization codes

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

12.6.4 Setting procedures

a) Object of the test

Verify that all procedures are in accordance with 8.2.3, setting procedures.

b) Principle

The test consists of setting the CIE using all the procedures provided as specified in the manufacturer's documentation and confirming that these are in accordance with the requirements within this specification.

Table 30 – Test of setting procedure

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
	<p>GENERAL CONDITION</p> <p>The CIE is in “unset” condition.</p> <p>For the purpose of this series of tests The keys and/or codes shall be selected to have the necessary authorisations for “inhibit”, and “override” functions.</p>		<p>GENERAL: Record the CIE condition</p>	<p>GENERAL CRITERIA</p> <p>When the CIE fails to set, means shall be provided to indicate or notify.</p> <p>If the indication of the set state is provided, it shall be limited to a maximum of 180s, after completion of setting.</p> <p>The logging shall be in accordance with 8.10</p>
<p>Complete the following series of tests for each setting procedure given in the manufacturers documentation, and for each fault signal or message specified in Table 4</p>				
1	<p>Alarm point (not allocated to an exit route) in active condition CIE unset</p>	<p>Try to set the system.</p>	<p>Record the CIE condition</p>	<p>The setting procedure shall be in accordance with Table 4 and 8.2.3</p>
2	<p>Alarm Point (not allocated to an exit route) in active condition Setting prevented (see step 1) CIE unset</p>	<p>Inhibit the active alarm point Try to set the system</p>	<p>Record the status of the CIE</p>	<p>The setting procedure shall be completed in accordance with Table 4.</p>
3	<p>The CIE in “unset” condition. Tamper signal or message applied to the CIE</p>	<p>Try to set the system.</p>	<p>Record the status of the CIE</p>	<p>The setting procedure shall be prevented in accordance with Table 4</p>
4	<p>Setting prevented (see step 3) CIE unset</p>	<p>Override the tamper Try to set the system</p>	<p>Record the status of the CIE</p>	<p>The setting procedure shall be completed, in accordance with Table 4</p>
5	<p>The CIE is in “unset” condition. Hold up signal or message applied to the CIE</p>	<p>Try to set the system.</p>	<p>Record the CIE condition</p>	<p>The setting procedure shall be prevented in accordance with Table 4</p>
6	<p>Setting prevented (see step 5) CIE unset</p>	<p>Inhibit the hold-up Try to set the system</p>	<p>Record the CIE condition</p>	<p>The setting procedure shall be completed, in accordance with Table 4.</p>
<p>For each fault signal or message specified in Table 5 repeat steps 7 and 8</p>				
7	<p>The CIE is in “unset” condition. Apply fault signal or message to CIE.</p>	<p>Try to set the system.</p>	<p>Record the CIE condition</p>	<p>The setting procedure shall be prevented in accordance with Table 4</p>
8	<p>Setting prevented (see step 7) CIE unset</p>	<p>Override the setting prevention</p>	<p>Record the CIE condition</p>	<p>The setting procedure shall be completed, in accordance with Table 4.</p>
9	<p>CIE is unset Setting sequence initiated Exit route timer running</p>	<p>Alarm point not allocated to an exit route activated.</p>	<p>Record the CIE condition</p>	<p>The CIE shall at least provide local indication and/or notification.</p>

12.6.5 Unsetting procedures

a) Object of the test

Verify that all procedures are in accordance with the requirements of 8.2.4.

b) Principle

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

Table 31 – Test for unsetting procedure

Step	Test condition (c)	Procedure (d)	Measurement (e)	Pass/fail criteria (f)
	GENERAL CONDITION The CIE is in "set" condition. The keys and the codes used are all valid with the necessary authority		GENERAL: Record the CIE condition	GENERAL CRITERIA When the CIE fails to unset, means shall be provided to indicate or notify. The indication of the unset state shall be limited to a maximum of 30 s, after completion of unsetting. The logging shall be in accordance with 8.10.
Complete the following series of tests for each unsetting procedure provided in the manufacturers documentation.				
1	CIE Set, in a normal condition with no alarms or, tampers activated.	Try to unset the system.	Record the CIE condition	The unsetting procedure shall be completed.
2	Alarm point (not on an agreed entry route) in active condition CIE set	Try to unset the system	Record the CIE condition	The unsetting procedure shall be completed. Notification and event recording shall comply with 8.2.4.3

12.6.6 Entry route and exit route facility

a) Object of the test

To verify that where entry and exit route facilities are provided, they conform to the requirements within 8.2.3.4 and 8.2.4.1.

b) Principle

Check the manufacturer's documentation, and where an entry route or exit route facility is provided, verify that the operation conforms to the requirements within this specification.

Table 32 – Test of entry route procedure

Test condition (c)	Action (d)	Check (e)	Pass/fail criteria (f)
GENERAL CONDITION Any Physical keys and/or logical codes are valid. Entry time set to maximum (not more than 45 s)			GENERAL CRITERIA Event logging shall be in accordance with 8.10
Complete the following test series for each unsetting procedure provided in the manufacturers documentation.			
CIE set	Start the unsetting procedure (entry time)	Record the CIE condition Record indication	The unsetting procedure shall be initiated. Indication shall be in accordance with Table 11 and Table 12
Unsetting procedure in process	Generate an alarm from an entry route alarm point, and complete the entry procedure.	Record the CIE condition Record indication and notification	CIE is unset. The intruder alarm shall not be processed. A correct entry procedure shall be indicated as per Table 11 and Table 12, and recorded in the Event log, optional for Grade 1, required for Grades 2,3 and 4.
CIE set	Start the unsetting procedure (entry time)	Record the CIE condition	The unsetting procedure shall be initiated
	Generate an intruder alarm from an entry route alarm point	Record the CIE condition	An intruder alarm shall not be notified.
	Do not complete the unsetting procedure (let the entry time expire).	Record the CIE condition	An alarm condition shall be notified according to 8.2.4.4
CIE set	Start the unsetting procedure (entry time)	Record the CIE condition	The unsetting procedure shall be initiated
	Generate a tamper alarm from an entry route alarm point	Record the CIE condition	The tamper alarm shall be notified
CIE set	Start the unsetting procedure (entry time)	Record the CIE condition	The unsetting procedure shall be initiated
	Generate an alarm from a non entry route alarm point	Record the CIE condition	Internal warning devices WD only, and indicator/s shall be activated, according to 8.2.4.3
Unsetting is proceeding	Wait 30 s after internal WD activated	Record the CIE condition	Where remote or external notification devices are connected, ensure remote or external notification is not activated prior to the completion of the 30 s in accordance with 8.2.4.3
	Do not complete the unsetting procedure (let the entry time expire).	Record the CIE condition	The alarm shall be notified in accordance with 8.2.4.4
CIE set	Start the unsetting procedure (entry time)	Record the CIE condition	The unsetting procedure shall be initiated
	Generate an alarm from a non entry route alarm point	Record the CIE condition	Internal warning devices and indicator shall be activated according to 8.2.4.3
	Complete the unsetting procedure (before the notification delay, see paragraph 2 of 8.2.4.3 time expires).	Record the CIE condition	The indicator and warning devices shall be restored and shall be not be notified The CIE shall be unset

Table 33 – Test of exit route procedure

Test condition (c)	Action (d)	Check (e)	Pass/fail criteria (f)
GENERAL CONDITION Set exit time	Allocate one or more alarm points to an “exit route”		GENERAL CRITERIA Event logging shall be in accordance with 8.10 The indications shall be in accordance with Table 11 and Table 12
Proceed to the complete test for each setting procedure given.			
CIE unset	Start the setting procedure (exit time)	Record the CIE condition	The setting procedure shall be initiated, and indicated according to 8.2.3.4 and 8.4.4
	Generate an alarm from an exit route alarm point, during the exit time period.	Record the CIE condition	The activated alarm point shall not cause alarm notification.
	Ensure the alarm point is no longer in the activated condition. Allow the setting procedure to complete.	Record the CIE condition	The setting procedure shall be completed. CIE is set, in accordance with 8.2.3.5 and 8.4.3
CIE unset	Start the setting procedure (exit time)	Record the CIE condition	The setting procedure shall be initiated, and indicated according to 8.2.3.4 and 8.4.4
	Generate an alarm from an exit route alarm point, during the exit time period.	Record the CIE condition	The activated alarm point shall not cause alarm notification.
	Ensure the alarm point is no longer in the activated condition. Allow the setting procedure to complete.	Record the CIE condition	The setting procedure shall be completed. CIE is set, in accordance with 8.2.3.5 and 8.4.3
CIE unset Exit procedure initiated Exit route alarm point activated	Exit route alarm point remains activated Exit time expires	Record the CIE condition	Incomplete exit condition indicated and/or notified, according to 8.2.3.6 CIE not Set No alarm notification

12.6.7 Event log

a) Object of the test

To demonstrate the ability of the CIE to maintain an event log, and keep an accurate clock.

b) Principle

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

c) Test condition

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

Table 34 – Test of event log

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
A	With the system unset and in the normal condition enter an authorisation code at each access level.	Note the facilities accessible to each access level.	There shall be no facility for a user to alter or delete the event log.
B	If the means of recording is cyclic: With the system unset, fill the event log. Add one more event	Note the 2 oldest events before the final event is added. Note the oldest event after the final event is added.	The oldest event shall be deleted by the last added mandatory events.
C	If the CIE has the facility to record non-mandatory events, then enter the appropriate number of mandatory events as defined in 8.10. Fill the remainder of the event log with non-mandatory events Add one non-mandatory event	Note the mandatory events recorded in the event log.	Verify that none of the logged mandatory events has been lost
D	Following the previous test (C), add one mandatory event	Note the mandatory events recorded in the event log.	Verify that the new mandatory event has been logged.
F	Remove PPS and APS from the system for a period of 30 days. At the end of this period, reapply power and check the event log.	Record the contents of the event log before removal of power, and after power is restored.	The contents of the event log shall not be lost or corrupted, (except for the inclusion of event(s) caused by this test procedure. (EXAMPLE:- Mains failure)
G	With the CIE unset and with no alarm condition, set the time and date.	Note the date and time.	
H	In CIE with the facility to make a permanent record, enter an authorisation code and initiate a permanent record.	Note the event log and the events recorded on the permanent record.	The events displayed on the permanent record shall accurately reflect the event log, including date and time.

	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
I	Where events are recorded at the ARC, check ability of CIE to send events to the ATE. Generate an event at the CIE	Monitor the output to the ATE.	Confirm that the generated events are sent to the ATE.
L	Where events are recorded at the ARC, check ability of CIE to indicate failure of transmission to the ARC. Disable the ATS and generate a number of mandatory events in accordance with 8.10, to be reported to the ARC. Enable the ATS	Record the indication and notification at the CIE, and the contents of the event log	For Grades 1 and 2 confirm a fault is indicated at the CIE. For CIE Grades 3 and 4, the CIE shall indicate a fault, and the event(s) shall be transmitted when the ATS is re-enabled.
M	Checking the clock accuracy.	When the system has been running for a minimum 8 day period note the indicated time by the CIE.	The accuracy shall be to within 50 s in 30 days

13 Environmental tests

The environmental test methods that shall be applied to CIE, are described in EN 50130-5.

NOTE The environmental test selection is reported in EN 50130-5, subclause 14.2.

13.1 General

The tests shall demonstrate that the CIE and any associated ACE will operate correctly during or after given environmental conditions without significant mechanical damage or degradation of performance. During operational tests there shall be no changes in status or generation of alarm conditions.

When the CIE and the ACE are declared with different classes (EXAMPLE: a class I CIE and a class IV external keypad), the severity of conditioning will be carried out for each device according to its declared class.

The CIE and ACE may be fixed, movable or portable, as defined in the manufacturer's documentation.

Prior to carrying out the environmental testing, a visual inspection shall be made to check for any mechanical damage. During the environmental tests the CIE shall be mounted, according to the manufacturer's specification, on a rigid support and connected to its PS enabling correct functionality.

The SD although electrically connected to the CIE, shall not be located within the CIE enclosure.

NOTE It is not the objective of this specification, or of this environmental test, to check the environmental functionality of the SD.

In the case of the vibration tests, an SD of typical size and weight, as specified by the manufacturer, shall be fitted according to the manufacturer's instructions.

The condition of the CIE and ACE shall be as specified in EN 50130-5.

13.2 Environmental test selection

Depending on the environmental class, tests shall be carried out in accordance with Table 35 and according to EN 50130-5

Tests shall be conducted in the following order on the sample indicated:

Table 35 – Environmental test selection

	Test		Sample number	Class I	Class II	Class III	Class IV
1	Cold	Operational	1	M	M	M	M
2	Dry heat	Operational	1	M	M	M	M
3	Dry heat	Endurance	1	-	-	-	M
4	Temperature change	Operational	1	M*	M*	M*	M*
5	Vibration	Operational	1	M	M	M	M
6	Free fall **	Operational	2	M	M	M	M
7	Damp heat. Cyclic	Operational	3	-	M	M	M
8	Damp heat. Cyclic	Endurance	3	-	-	M	M
9	Damp heat. Steady state	Operational	3	M	-	-	-
10	Damp heat. Steady state.	Endurance	3	-	M	M	M
11	Salt mist. Cyclic	Endurance	4	-	-	-	M
12	Water ingress	Operational	5	M*	M*	M	M
* = only for portable equipment ** = only for movable and portable equipment NOTE 1 Shock and Impact tests are covered by tamper protection requirements. NOTE 2 ESD and EMI tests are not covered by this document, as they are part of the related EMC Directives.							

Annex A
(informative)

Interconnection types

This Annex is intended to clarify interconnections.

A.1 Specific wired interconnections

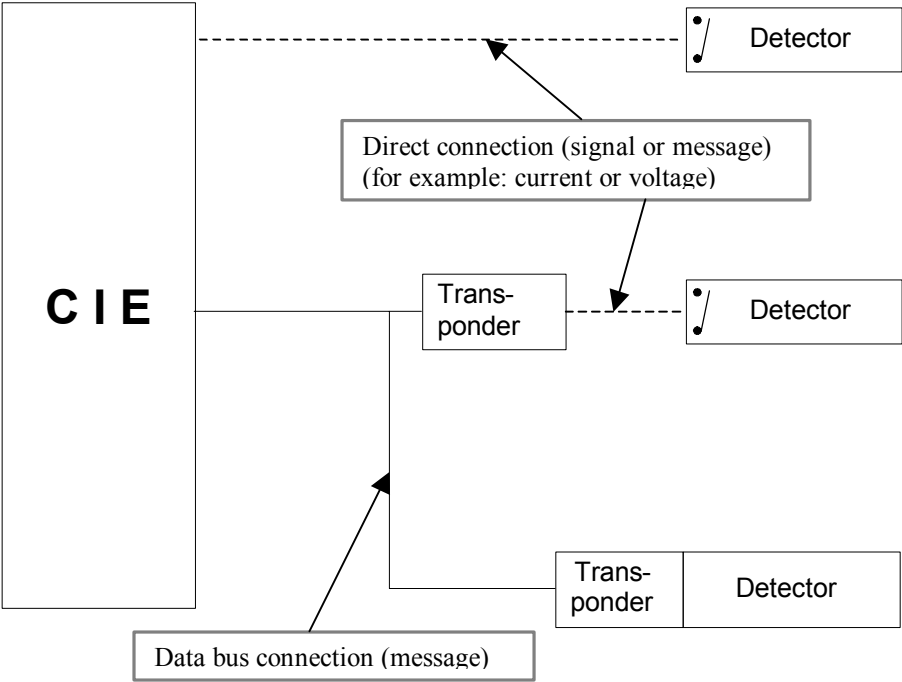


Figure A.1 - Specific wired interconnections

A.2 Non-specific wired interconnections

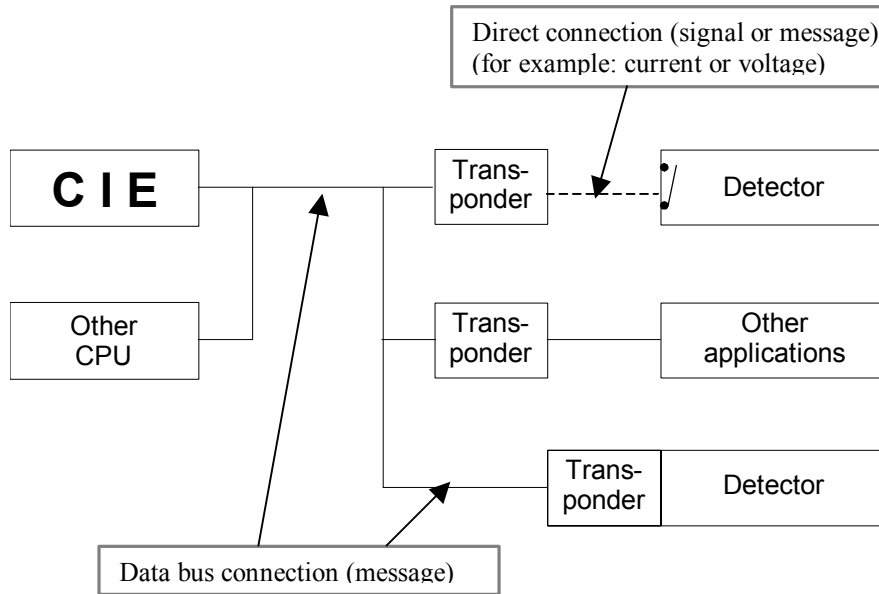


Figure A.2 - Non-specific wired interconnections

A.3 Wire-free interconnections

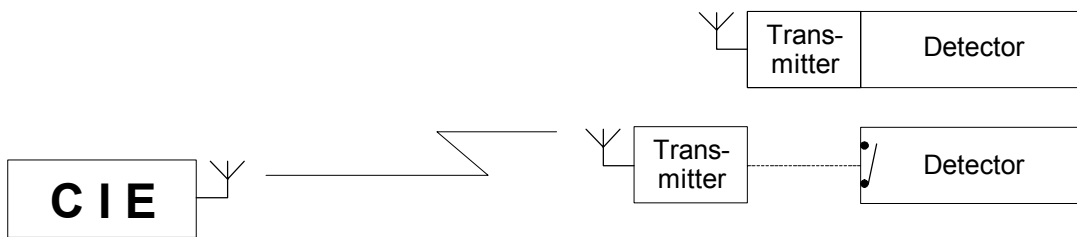


Figure A.3 - Wire-free interconnections

A.4 Timing of electrical signals

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

Annex B (informative)

Example of calculation for code variations

The number of logical keys can be calculated as:

Logical key variations = (number of different keys)^{code-length} - number of disallowed codes.

The manufacturer's documentation/information will show the number of combinations and number of disallowed codes.

EXAMPLE: When all authorization codes have length of 6 digits and an authorization code can consist of digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 then the number of combinations is $(10)^6 = 1,000,000$. If 0 is disallowed as the first digit, then the number of variations would reduce to 900,000. If 0 is not allowed anywhere in the code, the number of variations would reduce to $(9)^6 = 531,441$ combinations.

When different code lengths are permitted for each user, and the CIE automatically recognizes the code, then the number of combinations is calculated on the shortest permitted length.

When different code lengths are permitted, and the code is confirmed by the user (EXAMPLE: an Enter key), then the number of differs is the sum of the differs for each code length (EXAMPLE: 4, 5 or 6 digits and 10 different values for each digit $z=10^4+10^5+10^6$).

The test house will need the following information to perform the appropriate tests:

- number of bits or characters in the code;
- number of different values for each character;
- number of disallowed codes (EXAMPLE: several characters with the same value in the code (0000), sequence (1234), symmetrical codes (123321)).

Physical Keys

Interpassing the lock with normal keys. The elements necessary for the calculation will be given by the manufacturer:

- calculation of the number of theoretical differs;
- calculation of the number of effective differs according to the real manufacturing program;
- calculation of the number of effective differs after subtracting the differs dedicated to master-key systems;
- number of differs that can be opened with the same key.

These calculations should allow the test house to determine the minimum number of keys necessary to open all the locks likely to be distributed in Europe.

Opening the lock with fake keys:

A specific study for each model, the clearances and tolerances allow determining the following for each nominal depth of key bitting:

- the minimum height of the key bitting with which one can open a lock;
- The maximum height of the key bitting with which one can no longer open a lock

An intermediate bitting, midway between two dimensions, can open the lock and the bitting immediately above and the size immediately below.

A possibility of opening the lock with such a key reduces the number of keys required for opening all the locks of the model.

Annex C
(informative)

Summary of timing requirements

Table C.1 – Timing table

	Ref.	Process if more	Minimum	Maximum	Notify within
Intruder signal		400 ms	-		10 s
Hold up signal		400 ms	-		10 s
Tamper signal		400 ms	-		10 s
Fault signal		10 s	-		10 s
WD activation delay after the ATE		-	0	10 m	
WD duration			90 s	15 m	
EPS fault	Clause 8.3.1	1 h			
Main program watch-dog		100 s			
Memory integrity check			1 check per 24 h		
Duration of the "set indication" after SET				180 s	
Duration of the "unset indication" after UNSET				30 s	
Unsetting procedure duration				45 s	