EN 50131-1/IS1

Interpretation 1

EN 50131-1:2006

English version

Foreword

This interpretation of the European Standard EN 50131-1:2006 was prepared by Working Group 1 of the Technical Committee CENELEC TC 79, Alarm systems. The text of the draft was submitted to the Unique Acceptance Procedure and was approved by CENELEC on 2008-08-08.

EN 50131-1:2006, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*, includes many requirements that may not match traditional intrusion systems in some countries. Additionally, standards are written in a style which can make them difficult to understand unless some explanation is given. This interpretation is intended to provide extra information to readers of the standard to assist in its understanding. It should be read in conjunction with the standard.

This interpretation varies in the depth of detail provided. More detail is given for areas that prompted significant questions during the development of EN 50131-1:2006.

This interpretation may also assist translators by clarifying the meaning of the standard.

This interpretation is informative and the standard shall be used to resolve any disputes.

ATTENTION – Numbering of clauses and tables:

In this document (sub)clause and table numbers written in italic (e.g. *Table 7, Subclause 8.3.1*) refer to subclauses and tables in EN 50131-1:2006. Numbers written normally (e.g. Table 2, Subclause 6.1.1) usually refer to this document but, when specifically stated, may refer to other documents.

Contents

In clauses 3 to 9 of this document the section numbering matches the clauses of EN 50131-1:2006.

Only interpreted clauses are given and therefore the numbers are not continuous.

Attention: In this document *references in italics* refer to parts of EN 50131-1:2006

1 About this document

1.1 Scope

This document provides interpretation for the contents of EN 50131-1:2006 only. Other standards, technical reports or technical specifications in the EN 50131 series or EN 50136 series may be referenced but the interpretation is restricted to the scope and use of EN 50131-1:2006.

1.2 References

The standard that this document interprets is EN 50131-1: 2006, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements.*

Other standards referenced are those listed in the normative references of EN 50131-1:2006.

1.3 Definitions and abbreviations in this document

1.3.1 Definitions

The following definitions apply to terms used in this document that do not appear in EN 50131-1:2006. For other terms refer to EN 50131-1:2006.

1.3.1.1
alarm transmission equipment
equipment which is used primarily for the transmission of alarm messages from the supervised premises transceiver interface to the alarm receiving centre transceiver interface

NOTE This is based on definition 4.5 in EN 50136-1-1:1998. When used in this document it always refers to equipment that is part of the alarm transmission system located at the supervised premises, i.e. the supervised premises transceiver, whether housed separately or within another component of the I&HAS, e.g. the CIE.

1.3.1.2
duress situation
situation in which the I&HAS user is under direct threat and the triggering of an HAS should therefore be hidden from the attacker

1.3.1.3
identifier
physical or logical entity used by a user during authorisation (e.g. numeric code, proximity token, biometric characteristic, etc.)

NOTE The identifier does not necessarily uniquely identify a person.

1.3.2 Abbreviations

This document uses the abbreviations of EN 50131-1:2006 and the following.

ATE	Alarm Transmission Equipment

NOTE The abbreviation ATS (Alarm Transmission System) given in EN 50131-1:2006 is also used for the rating of ATS. In this instance it is followed by a number (e.g. ATS 4). Refer to *8.6.*

2 Brief guide on How to read the standard

2.1 Conventions used in standards (CENELEC Internal Regulations)

When reading standards, it is important to understand the relationship of the sections of the standard and to apply certain conventions. Ignoring these conventions may result in the reader misunderstanding the standard. For full details refer to "CEN/CENELEC Internal Regulations – Part 3: Rules for the structure and drafting of CEN/CENELEC Publications".

In particular:

- The "Scope" describes the limitations of the standard. In the case of EN 50131-1:2006 for example it states that it does not include "requirements for exterior I&HAS".
- A term defined in the list of definitions has only the meaning that is written in the list of definitions.
- Normative items are requirements. Informative items are advisory. Any item written as a note is informative.
- Things described as mandatory or written using the word "shall" are required by the standard. Things described as optional or written using the word "may" are not required by the standard but can be included by the I&HAS. If they are included in the I&HAS then they shall comply with any associated requirements.

The terms Permitted (P), Not Permitted (NP) and Not Applicable (NA) appear in the standard. "Permitted" means that the I&HAS may perform the action or include the function. "Not Permitted" means that for the given case the I&HAS shall not perform the action or include the function. "Not Applicable" means that the case should not occur. For example the I&HAS cannot indicate a set status when it is unset (*Table 9*).

In the remainder of this document the section numbering matches the clauses of EN 50131-1:2006.

Only interpreted clauses are given and therefore the numbers are not continuous.

3 Definitions

3.1.9 **alarm notification**

The use of the term "notification" within the standard also includes the use of warning devices and alarm transmission equipment with the objective of initiating an intervention by a response provider.

3.1.11 **alarm transmission system (ATS)**

This is one or more sub-systems used to transfer information about the I&HAS to one or more ARC. The standard is primarily concerned with the transfer of information about intrusion and hold-up alarms, fault and tamper conditions. The alarm transmission equipment (ATE) located at the ARC does not form part of the I&HAS. The ATS does not include transmission between components of the I&HAS with the exception of any interface between the CIE and the ATE.

3.1.12 **alert indication**

This only indicates that further indications are available. It gives no information specific to the event that causes it. It also does not imply that any condition causing the “further indication” is still present (see *8.5.3*).

NOTE 2 in *Subclause 8.5.1* clarifies that the alert indication may be suppressed in certain cases such as following triggering of a hold-up device.

The alert indication may have several forms. For example it could be audible and visual until acknowledged by a user and then become visual only, or the audible indication may be present if user response is required more urgently.

3.1.33 **interconnection**

An interconnection is a means of transferring information between I&HAS components. Interconnection does not refer to the system used to transfer information to the ARC (i.e. the ATS). The standard refers to three types of interconnection:

a) specific wired interconnection – an interconnection used solely for the transfer of information used by the I&HAS;

b) non-specific wired interconnection – an interconnection used by the I&HAS but also carrying information for other applications (i.e. any other system, e.g. a lighting control system or another I&HAS);

c) wire-free interconnection – an interconnection that employs a method of spatial transmission (e.g. radio frequency).

3.1.42 **masked**

A movement detector is “masked” when materials are accidentally or deliberately used to prevent the sensor from detecting movement in the intended detection area. This involves interference with the movement detector typically by the use of card, boxes or plates, close to the detector or spray over the surface of the sensor.

This differs from “significant reduction of range” in which the detector is still operational but detection is no longer possible over the whole of the intended detection area because of obstacles placed accidentally or deliberately within that area. The detector has not been directly interfered with but an intruder may move within the intended detection area without being detected.

“Masking” occurs close to the detector (e.g. within 50 mm) whereas “reduction of range” refers to a distance of several metres.

3.1.43 **message**

Each message carried by an interconnection may have a different meaning which is distinguished by the use of “function data”. The “function data” tells the receiver what the message means and provides the status or parameter values. The message may also include “identification” so that the source may be determined and other information for directing the message to a specific device and to determine whether it has been corrupted.

3.1.46 **non-specific wired interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.48 **notification**

The use of the term “notification” within the standard also includes the use of warning devices and alarm transmission equipment with the objective of initiating an intervention by a response provider.

3.1.49 **operator**

Whereas “user” (refer to *3.1.80*) is a person making use of an I&HAS at any access level (as implied by the definitions of hold-up alarm system, *3.1.28*, and indication, *3.1.31*) an operator is a user at access level 2, 3 or (less likely) 4.

3.1.53 **periodic communication**

“Periodic” means that in a pre-defined period at least one message should occur to ensure the interconnection is operational. A special message may be used to fulfil the timing but any message that is acceptable to the system is suitable.

3.1.61 **significant reduction of range**

Refer to the interpretation of *3.1.42* “masked” given above.

3.1.63 **specific wired interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.67 **supplementary prime power source**

This is a source of power that is similar to the prime power source and does not form part of the I&HAS but is used as an alternative supply for the supervised premises. An example would be a standby generator that automatically starts when the utility company’s AC mains supply is cut.

3.1.80 **user**

Refer to the interpretation of *3.1.49* “operator” given above.

3.1.83 **wire-free interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.84 **zone**

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

6 Security grading

The security grade should be chosen following a risk assessment. The methods of performing a risk assessment are beyond the scope of EN 50131-1:2006. The examples given in the note are simply guidance. Subclauses 7.1 and 7.2 of CLC/TS 50131-7:2008 describe aspects of risk assessment.

NOTE CEN Technical Committee TC 325 has drafted standards in the CEN/TS 14383 series that guide readers in the subject of risk assessment and grade selection.

7 Environmental classification

EN 50131-1:2006 uses the classification of environmental class given in EN 50130-5:1998. The latter describes how to test components and is for use by manufacturers. Installers and specifiers should select components with an environmental class suitable for the intended installation location. One I&HAS could include components of differing environmental classes. There is no relationship between environmental class and security grade.

8 Functional requirements

8.1 Detection

The requirements related to timing and signal durations are interpreted in *8.9*.

8.1.3 Tamper detection

Tampering may be detected in two ways: by components that include tamper detection as specified in *8.7.2* and as a result of the monitoring of interconnection requirements as specified in *8.8*.

8.1.4 Fault detection

EN 50131-1:2006 does not specify how component faults are detected. Those requirements are given in the component standards.

8.2 Masking and range reduction (also *8.4.5 and 8.4.6*)

Masking and movement detector range reduction detection is required at the grades specified. The methods of passing signals or messages indicating these conditions to components of the system are not specified. *Subclauses 8.4.5* and *8.4.6* permit the processing of these conditions to be performed as if they were either intruder or fault signals or messages. It is permitted to process these conditions as intruder or fault dependent on other circumstances (but this should be clearly described to users and the ARC). For example, a masking detection could be processed as if a fault when unset and as if an intruder when set.

The standard does not prevent additional responses (provided these do not interfere with the mandatory requirements). Examples could include procedures involving “walk tests”, etc.

8.3.1 Access levels

Subclause 8.3.1 and *Table 2* describe the four access levels and give requirements for relationships between them and the functions accessible to them. One important point is that it does not say that an I&HAS has four types of user. The access levels described are simply categorisations. When a function is shown in *Table 2* as “permitted” it does not mean that all users have access to that functionality. The access to a function can be restricted by user type (e.g. a cleaner may not be able to override a condition that prevents setting) or by restriction of a user to part of the IAS (e.g. the store man may be prevented from unsetting a high risk area). Access can also be restricted by circumstances (e.g. a guard patrol may be prevented from unsetting unless an alarm has occurred).

There are other requirements that restrict the access to functions of the system according to the authority granted to the user at that time. For example, *Sublause 8.5* refers to the indications available to different users. *Subclause 8.3.1* also contains many requirements about the access to functions.

In practice, an I&HAS may have many different types of user (e.g. the owner, the installer, a guard, a cleaner, etc.) but to simplify the description the standard uses four categories. The access level relates to the ability of a user at a specific time, however:

- the access levels are not hierarchical (e.g. access level 4 is not superior to access level 2);
- users may have authority to gain access at different access levels.

For example, “level 2 key or codes shall not provide access at level 3 or 4” does not mean that a user cannot have an access level 3 key or code that also permits them access at access level 2.

Access level 1 describes the operational restrictions applicable to a person who does not have any method of gaining authorisation (e.g. a shop customer or an intruder) or a person who has not currently identified himself to the system (e.g. the owner of a system before entering an identity code).

Access level 2 describes the operational restrictions applicable to a typical operator after authorisation by the I&HAS. They may set and unset the system but do not have any authority to change the way it works.

Access level 3 refers to the operational restrictions applicable to a person who has been recognised by the I&HAS and granted a higher level of authority. They should have some technical knowledge or in some way manage the use of the system and should have received sufficient training for this. Typically, this is the installer or maintainer of a system but could also be a manager of the system with the authority to control other users. Only access level 3 users have the authority to open the component housings without causing a tamper condition.

There may be access level 4 users. These are people who can significantly alter the operation of the system beyond simply changing configurable variables. Typically, this would be via a software upgrade of the CIE. The implication of this access level is that a special method exists to achieve this. It is not simply the replacement of a memory device by an installer because that could be performed by a user at access level 3.

Other requirements of the standard may restrict the ability of users according to security grade or circumstances. The requirements modifying *Table 2* are listed here:

Subclause 8.3.6 / Table 5	At higher grades some conditions cannot be overridden by users at access level 2
Subclause 8.3.9 / Table 6	At higher grades some conditions cannot be restored by users at access level 2
Subclause 8.3.11	Isolation is not permitted by access level 2 users on grades 3 and 4 I&HAS

8.3.2 Authorisation

Examples of “logical key” include a user code entered on a keypad, and an electronic card used with a proximity reader or a magnetic stripe card.

The authorisation stated in *8.3.2* applies in all cases when a user requires access to functions (whether it is for unsetting, viewing the event record, or changing site specific data, etc.). In each grade the number of differs can be the same for access levels 2, 3 and 4. *Subclause 8.3.4* permits all I&HAS to be set (but only set) using the number of differs of grade 1.

EN 50131-1:2006 requires that the functions listed in *Table 2* are restricted by use of authorisation techniques. There are three aspects to the authorisation:

1. the use of authorisation codes or equivalent means (as per *8.3.2*);

2. access to functions for users at access level 3 requires an access level 2 user to grant them permission;

3. access to functions for users at access level 4 requires access levels 2 and 3 users to grant them permission.

The standard does not specify when, or for how long permission is granted. Permission may be required on each attempt at authorisation, may be granted for a certain duration (e.g. for the next 8 hours), or for an indefinite period. This is however a standard for systems. It does not give procedural requirements. Therefore, the requirement is that the I&HAS is an integral part of the granting of permission (i.e. written authorisation is not sufficient).

Individuals use functions at certain access levels. Access levels are not attributes of the person. All users are considered to be using the system at access level 1 at certain times and, according to the authority granted to them, can then operate the system using alternative access levels. How this is achieved is not stated.

8.3.8.2 Unsetting

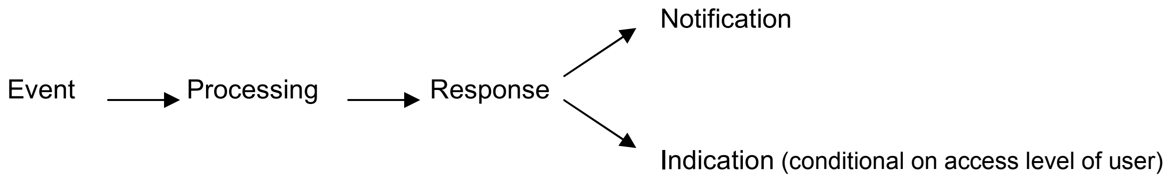
When this clause applies, remote notification (i.e. the transmission of messages to an ARC) is, depending on the sequence of events, possibly delayed by 30 s. If intrusion detection occurs after the end of the unsetting period (entry timer) but before the end of the 30 s delay, then the 30 s delay may be cancelled and ATS messages sent immediately.

8.3.9 Restoring

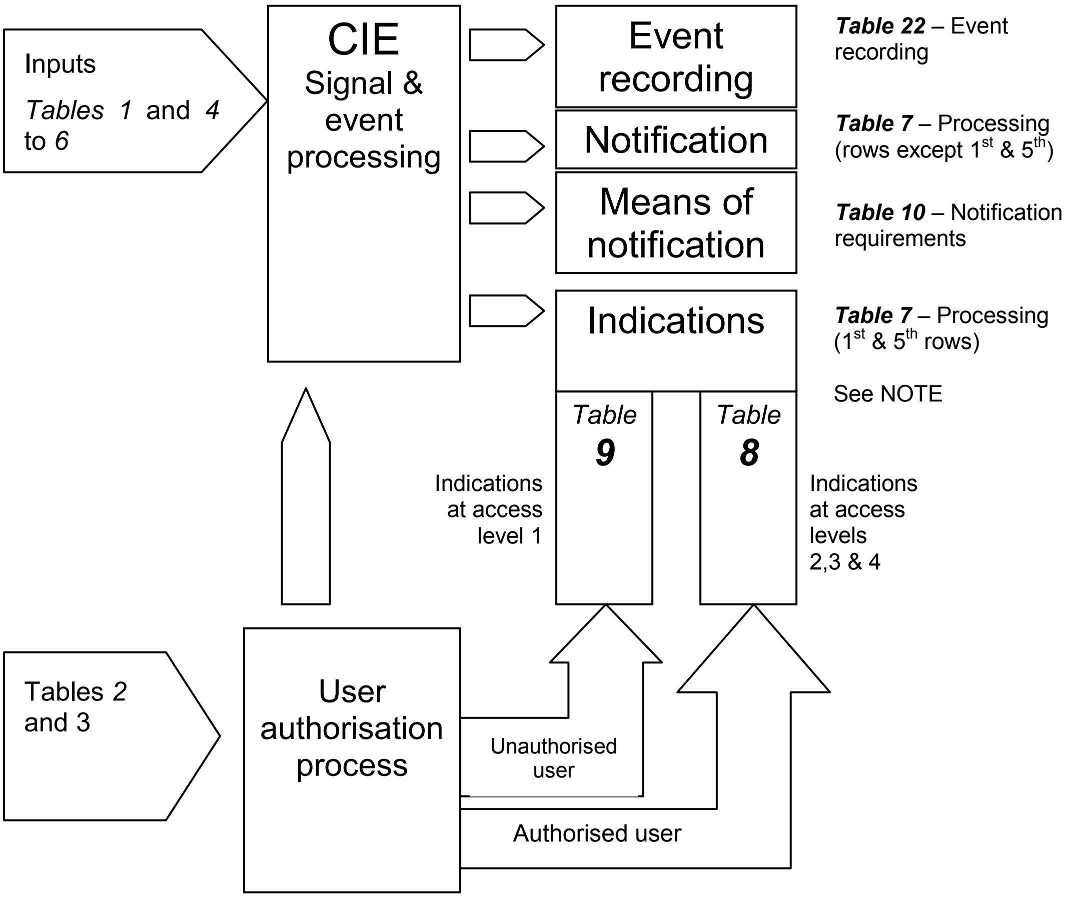
In *Table 6*, “Access levels 2 or 3” means that either access level may restore the I&HAS in accordance with the requirements of *8.3.9*. “Access level 2” means that the I&HAS should allow for one or more access level 2 users to restore the condition. Note that it is not mandatory to permit all access level 2 (or 3) users to have the ability to restore the I&HAS.

Subclauses 8.4, 8.5 and *8.6* - Processing, indications and notification

The three subjects of processing, indications and notification are very closely linked. Although the standard divides these items into three clauses they are related. For example, the requirements for “what” is notified are in *8.4, Processing*, rather than in *8.6* (which describes forms of notification). This interpretation views the system as being “event-driven”. That means that the processing begins as the result of an event and the outputs (notification and indication) are the result of the processing.



The requirements are detailed in the standard by the use of *Tables 7, 8, 9* and *10*. Figure 1 shows the relationship between these tables and the CIE. For simplicity of explanation this interpretation assumes that the processing functions of the CIE are centralised (this is the typical case) but distributed processing is permitted by the standard.


Inputs
Tables 1 and 4 to 6
CIE
Signal & event processing
Event recording
Notification
Means of notification
Indications
Table 22 – Event recording
Table 7 – Processing (rows except 1st & 5th)
Table 10 – Notification requirements
Table 7 – Processing (1st & 5th rows)
See NOTE
Table 9
Table 8
Indications at access level 1
Indications at access levels 2,3 & 4
Tables 2 and 3
User authorisation process
Unauthorised user
Authorised user

NOTE The indications shown in *Table 7* are restricted by the requirements of *8.5* (*Tables 8* and *9*).

Figure 1 – General processing

Events

All I&HAS are influenced by events of many types. Examples are detection of intrusion, a user unsetting the IAS, loss of AC power, etc. The standard gives requirements related to many events but cannot be expected to describe all possible events because of the diversity of products and their use. The following table links events to places in the standard where requirements are given.

Table 1 – Events – Cross references

	Referenced within *Table* number						
	1	***4 & 5***	***6***	***7***	***8***	***9***	***22***
Hold-up alarm (condition)		Y	Y	Y	Y		Y
Intruder alarm (condition)		Y	Y	Y	Y		Y
Tamper (condition)		Y	Y	Y	Y		Y
Faults	Y	Y	Y	Y	Y		Y
Zone/Intrusion detector/Hold-up device inhibited					Y		Y
Zone/Intrusion detector/Hold-up device Isolated					Y		Y
Overriding of prevention of setting conditions							Y
Zone/Detector overridden							Y
Changes to time and date							Y
Changes to site specific data							Y
Set					Y	Y	Y
Part set					Y	Y	Y
Unset					Y	Y	Y
Addition/Deletion of users							Y
Setting process					Y	Y	
Completion of setting					Y	Y	
Entry					Y	Y	
Completion of unsetting					Y	Y	
Failure to unset (8.3.8.2)							
Alert					Y	Y	
Key: Y = The table references the event							

8.4 Processing

Subclause 8.4, including subclauses, simply states that events are processed according to *Table 7*. Although *Table 7* of EN 50131-1:2006 includes reference to indications, it is primarily concerned with notification requirements. In terms of indications, *Table 7* merely states that all processed generic events shall cause an indication to be available (in this case to access levels 2, 3 and 4 users). It does not require indication at access level 1. The requirements for indications given in *8.5* take precedence over *Table 7*.

Table 7 Explanation

This interpretation uses the following excerpt of *Table 7* showing just grade 2 to allow explanation. The indication section has been removed for clarity.

Table 2 – Excerpt of *Table 7*

I&HAS Status	Outputs	Signals and/or Messages			
		Hold-up	**Intruder**	**Tamper**	**Fault**
Set	External Audible WD	Op	M	M	NP
	Internal Audible WD	Op	M	M	Op
	ATS Message Type	Hold-up [b]	Intruder	Intruder or Tamper	Fault
Unset	External Audible WD	Op	NP	NP	NP
	Internal Audible WD	Op	NP	Op	NP
	ATS Message Type	Op as Hold-up	NP	Op as Tamper	Op as Fault
Key: M = Mandatory, NP = Not Permitted, Op = Optional					
[b] Information relating to the Zone of the Hold-Up alarm to be included in the information transmitted to an ARC.					

Explanation

1. The column headed "I&HAS Status" refers to the status of the part of the system in which the event originates. If that part of the IAS is set then the upper part of the table applies. For Hold-up signals or messages the status refers to the status of the HAS. The IAS and HAS should be considered separately.

2. In some cases the status of the part of the system in which the event originates may be unknown (for example, an interconnection fault is detected in a part set system). In such cases the I&HAS should cause the most appropriate notifications permitted as are relevant to the current status of the I&HAS.

3. The column headed "outputs" refers to "External" and "Internal" WD. "External" means "not within the supervised premises". This does not necessarily mean outdoors.

4. The "ATS message type" refers to the type of message used in notification to the ARC.

5. The footnote "*b*" (relating to hold-up zone information) explains that there is a requirement for sufficient information to be sent to an ARC to enable them to direct an alarm response organisation (e.g. guards or police) to the correct part of the supervised premises. If no such differentiation is required for particular supervised premises then the extra zone information is not required.

6. The requirements of *Table 7* may be modified by other clauses of EN 50131-1:2006. These clauses are listed here.

8.3.8.2	Detectors located on an entry route can be ignored during unsetting.
8.4	Detectors can be logically grouped or multiple signals or messages required from individual detectors before being considered as a signal or message in *Table 7.*
8.4.1	After one intruder alarm condition has been notified, subsequent intruder alarm signals or messages need not be NOTIFIED. (Processing is required)
8.4.2	After one hold-up alarm condition has been processed, subsequent hold-up signals or messages during the next 180 s do not need to be PROCESSED.
8.5	The requirements for indications given in *8.5* take precedence over *Table 7*.

8.6 Notification by a WD may be restricted if its operation would cause it to exceed 15 minutes duration (or less if local or national requirements apply).

Notification by a WD may be suppressed if the ARC confirms it has received the notification message.

If an ATS is used, operation of the WD may be delayed by up to 10 minutes and during that time cancelled if the ARC acknowledges the message.

PPS fault notification may be delayed by up to 1 hour (and therefore may not occur if PPS returns prior to notification).

8.9.1 Intruder, hold-up and tamper signals shorter than 400 ms in duration need not be considered as a signal or message in *Table 7*. Fault signals shorter than 10 s in duration need not be considered as a signal or message in *Table 7*.

8.5 Indications (*Tables 7, 8* and *9*)

Table 7 of EN 50131-1:2006 states that, for intruder, hold-up, tamper and fault signals or messages, indication is mandatory. This however refers to the availability of indications to users at access levels 2, 3 and 4. The set and unset status refers to the status of the part of the IAS or HAS (as appropriate) from which the signal originates. The requirements for which indications must be available at access levels 2, 3 and 4 are given by *Table 8* and the restrictions for indications available at access level 1 are shown in *Table 9*.

8.5. General – [Indications at access levels 2, 3 and 4] (*Table 8*)

Only users that have been authorised at access level 2, 3 or 4 (see *8.3.2*) are permitted to view or hear information about the system other than that listed in *Table 9*. It is permitted to inform (visually, audibly or in any other manner) authorised users about any system information (regardless of whether the system is set or unset) but *Table 8* lists the items that the I&HAS must make available. See Table 3 below. *Subclause 8.5.1* states that it must be possible to perceive these indications from at least one single location but individual indicators may also be distributed throughout the supervised premises.

When the access levels 2, 3 or 4 user is no longer accessing the information of *Table 8,* it should become inaccessible to access level 1 users. This could be achieved, for example, by the use of a timer that clears a display after a short time.

It is not mandatory for all users to be provided with all indications. It is however mandatory (when an “M” appears in *Table 8*) for the I&HAS to make the indications available (how this is done is a matter for the equipment/system designer) to suitably authorised users. For example, a user with authority to set and unset only part of a system may be restricted so that information pertaining to other parts of the system is not available to them.

The alert indication (available to all users) informs authorised users that further information is available. Whilst viewing the further information, it is possible that yet further information is available. The user must be made aware of this by use of a “pending indication”.

The following table (Table 3) shows the association of the indications with certain attributes and the relationship between *Table 8* and *Table 9*.

The alert indication is the result of the availability of any indication (with the exception of the pending indication) that is not also available at access level 1. Although a “set” or “unset” indication at grades 3 and 4 fulfils these criteria, an alert is not permitted in these circumstances.

Table 3 – Contents of *Table 8* and *Table 9*

Indication	Time limited	Removed automatically	Remains until user restored (*8.5.3*)	Indication at access level 1 (all users) (from *Table 9*)								Indication at access levels 2, 3 and 4 (from *Table 8*)			
				Grade 1		Grade 2		Grade 3		Grade 4		Grade 1	Grade 2	Grade 3	Grade 4
				set	unset	set	unset	set	unset	set	unset				
Intruder alarm condition			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Individual intrusion detector indication [a]			Y	NP	NP	NP	NP	NP	NP	NP	NP	Op	Op	M	M
Intruder zone identification [a]			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Hold-up alarm condition [c]			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Hold-up zone identification [a c]			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Fault conditions (see *Table 1*)			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Tamper condition			Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Alert [b]		Y		NP	M	NP	M	NP	M	NP	M	M	M	M	M
Pending indication [b]		Y		NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
I&HAS set/ Part set	Y	Y		Op	NA	Op	NA	NP	NA	NP	NA	M	M	M	M
I&HAS unset	Y	Y		NA	Op	NA	Op	NA	NP	NA	NP	M	M	M	M
Inhibited	Y	Y		NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Isolated	Y		Y	NP	NP	NP	NP	NP	NP	NP	NP	M	M	M	M
Masking			Y	NP	NP	NP	NP	NP	NP	NP	NP	Op	Op	M	M
Range reduction			Y	NP	NP	NP	NP	NP	NP	NP	NP	Op	Op	Op	M
Setting (see 8.3.4)	Y	Y		NA	Op	NA	Op	NA	Op	NA	Op	Op	Op	Op	Op
Completion of setting (see 8.3.7)	Y	Y		M	NA	M	NA	M	NA	M	NA	M	M	M	M
Entry indication (see 8.3.8.2)	Y	Y		M	NA	M	NA	M	NA	M	NA	M	M	M	M
Completion of unsetting (see 8.3.8.2)	Y	Y		NA	M	NA	M	NA	M	NA	M	M	M	M	M

Key:
Y = This attribute applies,
M = Mandatory, NP = Not Permitted, NA = Not Applicable, Op = Optional ▨ NP = Not shown in standard (i.e. not permitted)

[a] These indications are merely providing greater detail about a generic event.

[b] The alert and pending indications are special cases that relate only to the availability of the other indications; they are therefore status related and automatically controlled.

[c] NOTE 2 of *Subclause 8.5.1* states that the alert indication may be suppressed in some cases.

8.5.2 Availability of indications [Indications at access level 1] (*Table 9*)

Table 9 lists all of the indications available to observers of the system who have not identified themselves to the I&HAS (i.e. a user at access level 1). No other indications are available. The requirements of *Table 9* are in some cases overridden by other clauses of EN 50131-1:2006. The following describes each item of *Table 9*.

Table 4 – Clarification for *Table 9*

Part of table	Clarification
"Time limited"	The expression "time limited" means that the indication is present during a particular procedure (e.g. setting) or for a limited time (e.g. a maximum of 30 s for completion of unsetting).
I&HAS set / Part set & I&HAS unset	As stated in the NOTE, at grades 3 and 4 no permanent indication of the set and unset state is permitted. At grades 1 and 2, it is permitted to have a permanent indication of the status. Although this indication may be provided using the same means as "completion of setting" (see below) it differs in that "completion of setting" is time limited (see *8.3.7*).
Setting	This permits the optional indication for setting included in *8.3.4*. The indication is only permitted whilst the setting procedure is in progress.
Entry & completion of unsetting	These indications are mandatory if the system is configured to operate as described in *8.3.7* option (*b*). Otherwise the requirement is optional.

8.5.4 Indication – Intrusion detectors

The aim of the requirement is that the IAS shall be capable of assisting users to identify the detector that generated the alarm condition. As examples, a PIR movement detector has processing capability and so that individual detector shall be identifiable by the IAS. A simple magnetic contact detector does not normally have processing capability.

To comply with *Table 8* and *Subclause 8.5.1* an indication (additional to that on the detector) must be located with the other indications "in at least one CIE or ACE". Also note that this indication is not included in *Table 9* and must therefore not be visible to unauthorised (access level 1) users.

8.6 Notification [Notification equipment] (*Tables 10 and 11*)

Table 10 specifies the minimum I&HAS configuration(s) for means of notification.

Manufacturers of CIE should provide the necessary interfaces to meet at least one of the options. That is the CIE should provide outputs for causing alarm transmission or activating warning devices and inputs for monitoring such equipment or alternatively such devices should be combined with the CIE.

Warning Devices (WD)

EN 50131-1:2006 specifies two categories of audible WD. They may be "Remotely powered" meaning that the WD does not contain a power supply to generate the sound and will therefore not sound if disconnected from the power source. The alternative type is "Self-powered" which means that the sound can be generated using a power supply within the WD. "Self-powered" WD may usually be powered from elsewhere, e.g. the CIE (to prevent discharge of batteries).

Alarm Transmission Equipment (ATE)

Table 10 refers to the performance criteria of alarm transmission systems using values ATS 1 to ATS 6. The scope of EN 50131-1:2006 is restricted to systems and components installed in or mounted on the exterior of the supervised premises (see *Clause 1*). The alarm transmission system (ATS) however extends from the supervised premises to the ARC and includes items of alarm transmission equipment (ATE) installed in both buildings. EN 50131-1:2006 therefore only gives requirements for the ATE installed at the supervised premises. The ATE satisfies the I&HAS requirements if it is capable of achieving the performance criteria stated in *Table 10* when connected to a suitable transmission network.

NOTE There may be additional requirements for the ATS to meet certain requirements of EN 50136-1-1:1998 but these do not form part of EN 50131-1:2006.

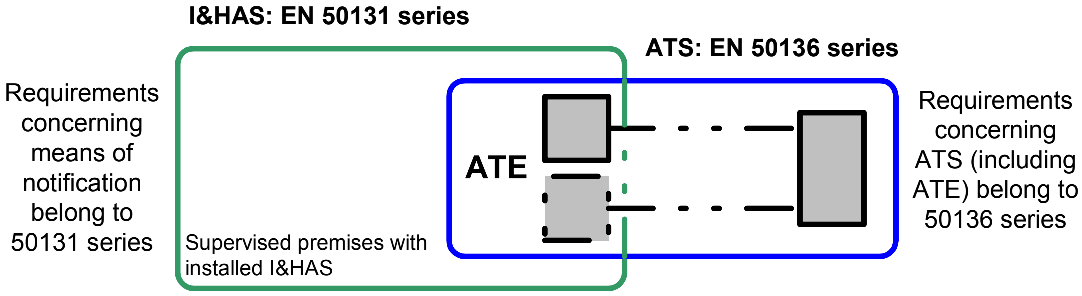

I&HAS: EN 50131 series
ATS: EN 50136 series
Requirements concerning means of notification belong to 50131 series
ATE
Supervised premises with installed I&HAS
Requirements concerning ATS (including ATE) belong to 50136 series

Figure 2 – Relationship of ATS and I&HAS

The reason why *Table 10* refers to ATS instead of ATE is because (at the time of its writing) there were no grade dependent requirements for ATE in any part of the EN 50131 or EN 50136 series. To differentiate the requirements for each grade the ATS performance criteria was used. The ATS rating (e.g. ATS 4) in *Table 10* refers to the criteria given in *Table 11*. The ATS ratings in *Table 11* are a selection from the generic performance criteria specified in EN 50136-1-1:1998 considered appropriate to I&HAS. These are summarised in EN 50131-1:2006, *Annex B*.

Note that EN 50136-1-1:1998 refers to an “Availability Classification” but EN 50131-1:2006 does not include requirements relating to availability.

It is recognised that in addition to tests of individual components it may be necessary to perform a test for type approval of an I&HAS [1]. If this is done then, although EN 50131-1:2006 includes specification of the ATS performance rating, it is not mandatory to test the ATS as part of the I&HAS type approval test. Separate testing of the ATS should be in accordance with the EN 50136 series of standards.

8.7 Tamper security

EN 50131-1:2006 gives overall requirements for tamper security and states these requirements “may vary” and protection should be “appropriate” It is not necessary to imply additional requirements because of these phrases. The detailed requirements and tests related to tamper security are described in the component standards.

[1] This may be required in some countries, particularly during the period prior to publication of relevant component standards (which at present are available as Technical Specifications, draft versions, or are not available).

NOTE Subclause 5.7 of EN 50136-2-1:1998 includes certain requirements for the protection of ATE including a phrase requiring the protection to be “the same as or higher than those of the associated alarm system”. Such requirements are found in the EN 50131 series component standards (for example CLC/TS 50131-3:2003).

8.8 Interconnections

8.8.2 Availability of interconnections

The note in *Table 16* describes the monitoring of RF frequencies for jamming and monitoring of interconnection buses for a similar lack of availability. In the case of a bus, this problem is most likely to occur with non-specific wired interconnections, as the result of a fault condition or because of an attempt to tamper the interconnection. Although this check can be performed at grades 3 and 4, the interconnection would simultaneously exceed the verification intervals for the interconnection integrity of *8.8.4.1* and *Table 17*.

A similar approach could satisfy the requirements at grades 1 and 2 but this might not be the optimum method. In most cases, the easiest way to check that the interconnection is available is to monitor it and check for sufficiently long periods (determined by the interconnection design) when it is not carrying a message.

8.8.4 Verification intervals

The communication referred to in *8.8.4.1* refers to each individual component of the system whereas the communication in *8.8.4.2* refers to any component (i.e. prior to setting at least one component must have successfully sent a signal or message within the period of *Table 18*. All components must have done so within the period of *Table 17*).

8.9 I&HAS timing performance

The time from detection of a condition (e.g. a detector detects intrusion) until the notification device is activated must not exceed 20 seconds. This is 10 seconds from *8.8.1* (maximum time allowed for the signal or message to go from the detector to the point of processing) plus a further 10 seconds. This further 10 seconds is the time in *8.9.2* concurrent with 10 seconds from *8.8.1* (maximum time for the signal or message to go from the point of processing to the notification device).

8.10 Event recording

Grades 2, 3 and 4 I&HAS shall possess some method of recording the events that have occurred for the purposes of fault diagnosis, proof of operation and forensic investigation. At grade 1 all aspects of the event record are optional.

Storage of events (*Table 21*)

Table 21 specifies the minimum length of time that the contents of the event record must remain uncorrupted in the complete absence of power (for example, after the end of the standby power supply period when the AC supply is disconnected). During this time, reconnecting power should enable recovery of all event records up to the time when power was lost.

The memory capacity stated in *Table 21* is the minimum number of the mandatory events listed in *Table 22* that can be simultaneously stored. If optional events are to be stored, they should not reduce the number of mandatory events recorded. How this is achieved is not specified by the standard (typically, larger storage would be provided or optional events deleted to prioritise storage). For example, if a grade 3 I&HAS with storage for 750 events also recorded the opening of a door in the unset state and the door was opened 251 times then some arrangement must be made to protect the storage of 500 mandatory events.

The deletion of stored events is only allowed under the automatic control of the I&HAS in order to store more recent events. There must not be a facility for users to delete records.

The standard requires that at least three events but no more than ten events shall be recorded from “a single source” during any set or unset period. This is to prevent the storage from being filled by repetitive events. A “single source” means one identifiable location (e.g. a detector) and the requirement applies to the same type of event. For example if twelve detectors employ a single tamper circuit but individual intrusion alarm circuits then no more than ten tamper signals should be recorded but an intrusion alarm could then be recorded from each detector in turn. The count is cleared when the I&HAS is set or unset.

Events to be recorded (*Table 22*)

Table 5 – Interpretation of some items of *Table 22*

Events listed in *Table 22*	**Provides supple-mentary information**	**Explanation**
User identity when setting/unsetting (when possible)	Yes	I&HAS employ two techniques to set or unset the system. One is identical for all users (e.g. a physical key) and therefore does not identify the user. The other should be different for each user (e.g. a numerical code). “When possible” implies that if the I&HAS uses the latter technique then it should record the identifier used. There is no guarantee that this identifies the user precisely.
Hold-up zone identification	Yes	Refer to explanation 7 in the interpretation of *Table 7*, Subclause 8.4
Intruder zone identification	Yes	Refer to interpretation of “zone” definition (3.1.84)
Individual intrusion detector identification (see *8.5.4*)	Yes	Refer to interpretation of Clause 8.5.4
Interconnections fault		Whilst the term “fault” is used, it is recommended that tampers caused by interconnection problems are equally recorded (see below).
Detector first to alarm	Yes	The first detector to cause an alarm may be determined by the order of recorded events. It is suggested that this record may require additional protection. For example, maybe it should not be deleted until after the alarm condition is restored.

When *Table 22* lists the start of a condition as mandatory, it is recommended that the subsequent removal of that condition should also be recorded. For example, “intrusion detector isolated” is listed but not “removal of intrusion detector isolation”. Failure to do this would result in the event record apparently showing repeated failures without recovery.

Although *Table 22* states that the optional or mandatory nature of an event record is dependent upon the grade of the I&HAS, any event listed as mandatory in a higher grade can be considered as mandatory in a lower grade for the purposes of determining the deletion or protection of events as described above. For example, if “Prime Power Source Fault” is recorded by a grade 2 IAS then it is not required to delete that record for the purposes of storing an event listed as mandatory at grade 2 in *Table 22*. This permits the use of grade 3 CIE within a grade 2 I&HAS without additional configuration.

Recording events outside the I&HAS

Transfer of the event record to the ARC is useful but it is recommended that this is used in addition to storage within the I&HAS. This may be particularly useful if a system records a large number of optional events. Storage within the I&HAS is always required and should comply with the requirements stated in *8.10*.

The intention of the note in *8.10* is to recommend that recording at the ARC should provide storage meeting the clause requirements for each connected system.

Permanent record of events

Grades 3 and 4 I&HAS shall offer a facility to transfer the contents of the event record to another format or system with greater endurance. Examples could be a print copy, electronic or optical storage. This could be achieved locally or by transmission to a remote location. It is only the transfer facility that is required not the means of printing or storage.

9 Power supply

For a full understanding of power supply requirements it is recommended that EN 50131-6 is read.

Any power supply that consists entirely of finite capacity power sources (such as batteries) should be considered to be a type C power supply. Type C power supplies should be capable of providing the necessary power for a minimum of one year following installation of the storage device.

It is recognised that the change over from the prime power source to alternative power source will be accompanied by the existence of a prime power source fault condition but the change over should not cause spurious alarm conditions.