bsia
british security industry association

guideline for the use of
the PD6662:2010 scheme for I&HAS standards

March 2011

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 271 Issue 1

1. Introduction

PD6662:2010 is the foundation document in the UK for the implementation of European Standards for Intruder Alarm Systems and is based on the revised BS EN50131-1:2006, including Amendment 1:2009.

This document has been prepared to give guidance on the interpretation of some of the clauses in PD6662:2010 and BS EN50131-1:2006+A1: 2009 that may be open to misinterpretation or in need of further clarification. It must be read strictly in the context of the scheme outlined by PD6662:2010. This document may be updated as circumstances require.

Only those items in PD6662:2010 and BS EN 50131-1: 2006 which give concerns are listed below. All other clauses or parts of the standard are believed to be self-explanatory.

Whilst prepared initially for use by manufacturers when designing products to conform to the new requirements, this guideline should also be a useful source of clarification for specifiers, installers and others working with the standard.

This document was made available for use by the industry by the BSIA Manufacturers Technical Committee (TC/1).

Similar guidelines have been produced by BSIA for each of the available product / service standards, which include standards change guidance – see below:

Form 279 Guidelines to the alignment of BS EN 50131-3: 2009 Alarm Systems – Intrusion Systems Part 3: Control and Indicating Equipment with BS EN50131-1:2006+A1:2009

Form 280 Guidelines to the interpretation of BS EN 50131-6:2008 Alarm Systems – Intrusion Systems – Part 6: Power Supplies

Form 104 Guidelines to scenarios related to BS8243:2010 Clause 6.4.5

Form 175 Industry agreement on the implementation of additional communications requirement between ATE and CIE

Form 294 Summary of changes between 2003 & 2008 versions of DD CLC/ TS 50131-7

Form 295 Changes introduced under DD263:2010 (as compared to PD6662:2004)

Form 296 Summary of changes between PD6662:2004 & PD6662-2010

Form 297 Summary of changes between BS8243 and DD243:2004

Form 327 User guide to I&HAS incorporating sub-systems

Form 270 Summary of changes to EN50131-1

Note: Some of the above documents are available only to member companies.

Referenced documents

BS 8243: 2010 – Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions – Code of practice.

BS 8473: 2006+A1:2008 – Intruder and hold-up alarm systems – Management of false alarms – Code of practice.

BS EN 50131-1: 2006+A1:2009 – Alarm systems – Intrusion and hold-up systems – Part 1: System requirements
BS EN 50131-2 series – Component standards suite.

BS EN 50131-2-4: 2008 – Alarm systems – Intrusion and hold-up system – Part 2-4: Requirements for combined passive infrared and microwave detectors.

BS EN 50131-2-6: 2008 – Alarm systems – Intrusion and hold-up systems – Part 2-6: Opening contacts (magnetic).

BS EN 50131-3: 2009 – Alarm systems – Intrusion systems – Part 3: Control and indicating equipment.

BS EN50131-5-3: 2005+A1 : 2008 – Alarm systems – Intrusion systems – Part 5-3: Requirements for interconnections equipment using radio frequency techniques.

BS EN 50131-6: 2008 – Alarm systems – Intrusion systems – Part 6: Power supplies.

BS EN 50136 series – Alarm transmission systems and Equipment suite.

DD 263:2010 – Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice.

PD 6662: 2004 – Scheme for the application of European standards for intrusion and hold-up alarm systems.

PD 6662: 2010 – Scheme for the application of European standards for intrusion and hold-up alarm systems.

prEN 50131-1: 2004 – Alarm systems – Intrusion and hold-up systems – Part 1: System requirements.

Note: prEN50131-1: 2004 is only valid in the PD6662: 2004 scheme; it is referenced here as comparisons are made within this document.

Form 175	Industry agreement on the implementation of additional communications requirement between ATE and CIE
Form 280	Guidelines to the interpretation of BS EN 50131-6:2008 Alarm Systems – Intrusion Systems – Part 6: Power Supplies
Form 327	User guide to I&HAS incorporating sub-systems

Interpretation of clauses:

PD6662:2010 Clause 4.2 – Documentation

Although not fully in accordance with parts of EN 50136, the following practical approach is suitable for declaring the performance characteristics of ATS in the UK. The SPT manufacturer's statement of conformity shall declare that, with the specified transmission network functioning normally, the ATS will comply at the stated performance level, subject to the ARC being adequately equipped.

The clause and table numbers used from this point refer to EN50131-1:2006 including A1:2009, unless otherwise stated.

Clause 3.1.12 – Alert indication

This clarifies that, except for indications specific to the setting / unsetting procedures, this is the only indication permitted at level 1 (see table 9). The definition draws attention to the fact that specific information is available to a level 2 (or higher) user, as described in 8.5.1. An alert may be visual or audible, and if given by a warning device should be easily distinguishable from an alarm (e.g. two different tones or distinct volume levels). Status indications available to access level 1 users are not permitted, for example on detectors and power supplies.

Clause 3.1.42 – Masked

The EN 50131-2-x series of movement detector equipment standards define the masking requirements for individual types of detector.

Clause 3.1.51 – Part Set & Clause 3.1.65 Subsystem

EN 50131-1 states that a subsystem is "a clearly defined area of the supervised premises". The recommendations of BS 8243: 2010 Clause 6.4.1 "apply to each subsystem configured to generate a confirmed alarm if set in isolation from the remainder of the IAS." This means that to be considered as a "subsystem" the design should include an unsetting method for each subsystem from BS 8243 (i.e. a choice of 6.4.2 to 6.4.6). In other cases the method of setting would be considered a "part set". Whilst it is considered appropriate for subsystems compliant to BS 8243 to be capable of gaining police response this may not always be the case for part set systems.

Refer to BSIA Guide Form 327 for more information about subsystems.

Clause 3.1.55 – Prime power source (PPS) & Clause 3.1.67 Supplementary Prime Power Source (SPPS)

Note that these terms should be read in conjunction with the more detailed description in EN50131-6:2008, which also uses the term "External Power Source (EPS).

Clause 3.1.82 – Warning Device

It should be noted that the new definition of "warning device" excludes visual devices e.g. strobes. A strobe should be treated as a supplementary device.

Clause 7 – Environmental Classification

Components shall be suitable for the environment for which they are to be used. This includes junction boxes, which, in the absence of a product standard, should be subjected to the same environmental tests as shown in the detector standard EN 50131-2-2, tables 7 and 8.

Clause 8.1.4 – Table 1 Recognition of faults

Reference requirement for "ATS fault" (Note that in the terminology of EN 50131-1 "ATS" is used for both a transmission path and a combination of paths).

a. Table 1 of BS EN 50131-1 requires an ATS fault response to be given from a failure of ANY ATS path – though does not require identification of which. BS EN 50131-1 also requires a number of responses to ATS faults (e.g. Table 4 note b, Table 5 note b, 8.6 paragraph 6, Table 22). Regarding prevention of setting, "both a loss of ANY path" and "loss of ALL intended signalling paths" are required to generate a response.

   It is therefore essential for information indicating a fault with any or all paths to be exchanged between SPT and CIE.

   One method of achieving this using a limited "pin" type interface, compatible with older equipment, is described in BSIA Form No. 175. Other methods may be employed.

b. BS EN 50136-1-1 defines criteria for ATS faults. It is also possible for the SPT or CIE to recognise a fault in other conditions (e.g. a failure of the interconnection between the SPT and CIE, failure of power to the SPT, etc). ATS faults may be the result of:

   i. Failure to achieve transmission of an alarm or other message within the ATS performance requirements, or
   ii. Determination of a fault of the alarm transmission path by monitoring (e.g. by polling, PSTN voltage measurement, etc).

   In the case of (ii) it should be recognised that the fault may not prevent the transmission of an alarm within the required time, i.e. a fault of type (i). Many methods of alarm transmission suffer temporary faults that, if indicated to the user of the I&HAS, would cause undue concern or result in the user ignoring faults of genuine concern. It is therefore considered appropriate to delay the indication of faults (and subsequent restore requirement, as per clause 8.3.9) caused by monitoring failures, i.e. a fault of type (ii). Refer to the description in this document of "Condition Developing Phase" in the comments on clause 8.9.1. Any such delay in indication should not affect other required responses of EN 50131-1, especially the prevention of setting.

c. Prior to the implementation of EN 50136-1-1, systems frequently determined an alarm transmission fault following a number of attempts to transmit an alarm. However, EN50136-2-3 clause 5.3.6 states that a fault signal should be generated from the ATE to the I&HAS in the event of "failure to achieve a successful connection and / or transmission of the information message within 240 seconds." Whilst EN50136-2-3 specifically relates to digital communicators using the PSTN, where there is an absence of similar requirements in standards relevant to other network types, this is considered an appropriate maximum for all types of system for communication to an ARC.

Clause 8.2.1 – Masking

Detection of masking of movement detectors is mandatory in Grades 3 and 4. It should be noted that Table 2 of the BS EN 50131-2-x movement detector standards states that masking may be signalled from the detector as an independent signal, or by signalling "intrusion" and "fault" simultaneously.

Clause 8.3.1 – Access Levels

The requirements related to authorization at different access levels should take into account Annex A.3 of PD 6662: 2010. These requirements are also relevant to access during "remote support" or "remote system checks" in accordance with DD 263: 2010. This means that such remote access at level 3 similarly does not require authorization on each separate occasion provided that a written agreement exists. The requirements of Clause 4.2 of DD 263 still apply.

Clause 4.2 c) option 3 of DD 263 requires a user on site to complete the initialization of remote access. This process should take into account indication requirements of clause 8.5 of EN 50131-1 and therefore may necessitate the authorization of the user (e.g. by use of a PIN) so that they can be aware that remote access is being attempted.

Table 2 Level of access

Note 1 within Table 2 identifies that not all functionality is mandatory. If the facility for a manufacturer to change/ replace the basic programme whilst the system is operational is not provided, then there is no need for Access Level 4 to be provided.

Clause 8.3.4 – Setting

a. Table 2 makes it clear that users at level 3 can only set if the appropriate authorisation (level 2) has been given. See 8.3.1 above.

b. It is permitted to use a 3-digit code to set for all grades of system.

c. The requirement for each user to be individually identified is shown in table 22 as "when possible," hence having multiple users of the same PIN code (or key) is permissible at all grades (though not good practice).

Clause 8.3.5 – Prevention of setting

a. The clause lays out the conditions that should cause the prevention of setting of the I&HAS. The condition causing the prevention of setting should be relevant to the part of the I&HAS being set.

b. The prevention of setting condition should be assessed by the processing both at transition from unset to starting set and at completion of setting.

c. BS EN50131-1 does not specifically require monitoring of the prevention of setting condition throughout the setting period, but BS EN50131-3:2009 (clause 8.3.3.1) requires a warning to users if prevention of setting takes place, Hence, whilst exit strays are allowed as long as all detectors have settled down at the completion of setting, they must be monitored throughout.

d. If an interconnection problem is identified as a fault then it should be processed as a fault, but if it cannot be identified as a fault then it should be processed as a tamper (see 8.8).
See also comment in PD6662:2010 referring to clause 8.8.

Clause 8.3.6 Overriding prevention of setting

It should be noted that it is not necessary for equipment to include the ability to override prevention of setting. In some instances it may be judged inappropriate to allow users to override. This means that a user may not always be able to override and setting will therefore be prevented.

Clause 8.3.8.2 – Unsetting – as specified in clause 8.3.7b.
(See BS8243:2010, Annex G for entry timelines, which clarify this clause)

a. This clause requires an entry indication, which may be audible or visible.

b. In the event of an alarm condition being generated during entry time (e.g. by deviation from the entry route), a local indicator or WD is required for at least 30 seconds and entry time must have expired before remote notification is permitted.

   If the system is unset during the 30 seconds then notification should be cancelled.

c. If the entry timer times out and no other alarm condition has occurred (i.e. straying from the entry route) an alarm condition can be notified immediately, i.e. unlike under prEN50131-1: 2004 there is not a 30 second delay in remote notification in these circumstances. See BS8243 Annex G timing diagrams.

d. For systems including alarm confirmation according to BS 8243: 2010, Clause 8.3.8.2 directly relates to Clause 6.4.5 of BS 8243. It should be noted that police forces may restrict the use of this unsetting method in combination with the use of duress PINs. A duress PIN unsets the system whilst also secretly notifying the ARC that the user was coerced. As unsetting method 6.4.5 of BS 8243 prevents the use of a PIN for normal unsetting of the system the use of a duress PIN is questionable. In England and Wales, ACPO will only permit duress PINs in grade 4 and with individual permission at grade 3 and not in combination with unsetting method 6.4.5.

Clause 8.3.9 – Restoring

Restore of a condition specified in Table 6 is permitted by an ARC providing an "anticode" to a level 2 user at the supervised premises, provided that this "anticode" meets the number of differs required by Table 3 (see also BS8473:2006 and DD263:2010).

Clause 8.3.9 – Table 6

a. In table 6 it shows that for Grades 3 and 4 access level 3 ("engineer") is required to restore a system following a tamper.
b. The restore of sequentially confirmed alarm conditions passed to the police in accordance with BS8243 must be carried out by the alarm company's service technician or in conjunction with the Remote Monitoring Centre (RMC) at all grades (see BS8473).

Clause 8.3.10 Inhibit operation and 8.3.11 Isolate operation

Both clause 8.3.10 and clause 8.3.11 talk about "functions". A function is detailed at clause 4 of BS EN50131-1 and cross referenced in BS EN 50131-3 clause 8.3.6 and clause 8.3.7.

Table 22 shows that both inhibit and isolate operations are not restricted to "functions," but may be applied at individual detector level.

Clause 8.3.12 – Test

This clause states that there is a requirement to carry out a functional test of hold-up devices. The clause does not specify that notification (remote or local) is part of the test, therefore it is agreed that the hold-up test may be indicated or locally or remotely notified. Security during the test is the responsibility of the user. If the user wishes to include remote notification in a hold-up test, then they should advise the ARC prior to the test.

Clause 8.4 – Processing

In identifying the use of "pulse counting" at detectors, the 4th paragraph of this clause does NOT mean that "double knock" cannot be applied at the CIE. The 3rd paragraph identifies a CIE function in logically grouping multiple responses from a single detector (ie "double-knock") or responses from multiple detectors in order to generate an alarm condition.

Clause 8.4.5 – Masking signals or messages

This clause specifies that "masking" may be processed as a "fault" OR as an "intruder," thus Table 7 does not separately itemise responses for this condition.

All required responses can be achieved by processing masking as an intrusion. It is therefore recommended that this be done.

Notes:

1. Provision of the "masking" output from movement detectors when the IAS is unset is mandatory according to the requirements in BS EN 50131-2-x movement detector standards. This does not allow for the message to be delayed until the point of attempting to set the I&HAS.

2. Provision of the "masking" output from movement detectors when the IAS is set is NOT mandatory according to the requirements in BS EN50131-2-x movement detector standards. It is recommended that the output be used, and be processed as an "intrusion" signal. Where this is done, BS8243 does not permit intrusion and masking events from the same detector to qualify as a sequentially confirmed alarm.

3. Note that BS EN50131-3:2009 clause 8.1.6 contains an error (which Cenelec secretariat will correct in due course. The last paragraph should read:

   "The CIE shall process masking signals or messages when the system is unset and optionally when set."

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

a. The "Indication" row in table 7 gives information to help the user in the operation of the system and is available to level 2 users at any time after they have entered their access code.

b. Hold-up messages may be notified when the HAS part of the I&HAS is set and the IAS part of the I&HAS is in any state.

c. The table shows that system faults and system tampers are to be treated differently, but does not differentiate how a system will differentiate between a wiring fault and a tamper. This is dealt with under clause 8.8.4.1 and Table 20, if there is no means of differentiation it will be treated as a tamper.

d. In the event of a failure to set what can the system do to alert the user? EN50131-3:2009 clause 8.3.3.3 requires that means be provided to indicate and/or notify such an event. The standard allows for an alert indication (which may be audible) and/or transmission of a failure to set signal to an ARC. A failure to set may be considered as a fault and if so, should be processed accordingly (which permits remote notification).

e. There remains some uncertainty over the requirement stated by the note b in the table, as it seems to intimate that an individual detector location would need to be signalled.

It must be remembered that a zone, as used in BS EN50131-1:2006, is not an individual detector/device. "Zone" is defined as "an area of the supervised premises where an intrusion, attempted intrusion, or the triggering of a hold-up device may be detected ". This also means that Fast Format can be used to send hold-up zone information – subject to there being sufficient channels available to provide the necessary differentiation.

f. This table permits the use of an "intruder" signal to convey "fault" information to the ARC whilst the IAS is set, in grade 1 and 2 systems.

   This should NOT be done in systems required to comply with BS 8243:2010 in order to minimise false alarms.

Clause 8.5.1 – Indications – General

a. 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.

b. Table 8 shows the indications that are mandatory. However, these can be made available only to Access Level 2 users and above, except those indications shown at Table 9, which can be shown to Access Level 1 users. Note 2 allows indications to be suppressed in certain cases, for example Hold-up.

c. EN50131-3:2009 table 6 identifies additional indications that are required.

Clause 8.5.2 – Availability of indications – Table 9

a. Indications permitted by Table 9 are available at Access Level 1 – i.e. to any person. Those in Table 8 are only available to users at access level 2 or above.

b. Table 9 states that an alert cannot be displayed whilst the system is set, yet Table 7 states that signals should be indicated when the system set. It must be remembered that the indications in Table 7 do not include the alert. This is clarified by the note in clause 8.5.3.

c The alert indication is normally displayed at level 1 as soon as the I&HAS is unset, as per 8.5.1 and Table 9. It is permissible to display the first non-alert indication immediately at the point of unset (but not elsewhere), as an access level 2 user has just entered their code.

Clause 8.5.3 – Cancelling indications

a. The indication resulting from a specific condition must remain available to a level 2 user until manually cancelled AFTER the condition has been cleared. Remember other indications as specified in Table 8 should not be available to an access level 1 user (as per the note) except for a set status indication if BS EN50131-1 clause 8.3.7 option c) is used (grades 1 and 2 only).

b. This implies a time limit to the level 2 indication. It is agreed that different methods may be used e.g. a time limit, a manual function, a warning tone informing the user the indication is still present, etc.

   When the level 2 access is cancelled in this way, the "alert" indication again becomes valid.

Clause 8.5.4 – Indications – Intrusion detectors

a. EN 50131-1 specifies that the detector must have means of indication of an alarm condition. The EN 50131-2-X series of standards requires detectors to have indicators but does not require them to be enabled. Use of this indication at the detector is not permitted at access level 1, in accordance with clause 8.5.2 and Table 8.

b. Because of the requirements of 8.5.1 paragraph 4 and Table 8, all detectors including processing capability must be separately indicated at the CIE at Grade 3 and 4.

Note: PD6662: 2010 clause C.1 defines what is meant by "detectors, which include processing capability."

Clause 8.6 – Notification, Table 10 & Table 11 (Annex B)

a. Paragraphs 5 and 6 allow for a WD delay period with the possibility of permanent suppression of the WD. The delay is dependent on the absence of any fault in the ATS transmission path. The suppression is dependent on confirmation to the CIE from the ARC of receipt of the signal being received during the WD delay period.
b. Suppression of the WD is also permitted (para 3) for events such as a Hold Up Alarm.

c. The use of a WD delay with entry deviation and entry timeout alarms is NOT recommended.

d. Paragraph 8 of the clause talks about the notification of prime power faults. A single fault message type may be used for remote notification. This may indicate all faults including primary power faults, but in grade 3 and 4 systems separate notification of a primary power source fault will be required to permit 50% reduction in the capacity of the standby power supply.

Clause 8.7.2 – Tamper detection

From Tables 12 and 13 the requirements for ACE can be seen to include detection of tamper when opened by normal means. Note that Clause 8.7 of EN 50131-3 categorises ACE into Type A and Type B. Type A is categorised as "Access to internal elements resulting from damage to the housing could not enable the status of any part of the I&HAS to be changed or prevent the initiation of mandatory notification". The implication of this is that tamper detection for the normal opening of a Type A device is not required. This is confirmed by footnote 'a' in Table 8 of EN 50131-3. An example of a type A device is one that is fully potted.

Clause 8.7.3 – Monitoring of substitution

In a Grade 4 system all components should be uniquely identified to the system and attempts at substitution detected as specified. The term "components" refers to detectors, keypads, etc (see table 12) – not to electronic components such as resistors, capacitors, etc.

Clause 8.8 – Interconnections (wired only)

Whilst considering the requirements for interconnections it must be remembered that identification of individual intruder detectors is not required at grade 1 and 2 (table 8 refers), implying that this would also be true for tampers. Also looking at interconnection tamper requirements and the grading definitions stated in clause 6 the following should apply, as a minimum:

a. Grade 1 – Double pole – Common tamper
b. Grade 2 – Double pole, End of line, etc – common tamper is acceptable
c. Grade 3 – Double pole, End of line, etc – individual tamper is required, iD or similar system
d. Grade 4 – System with unique identities.

Note: Attention should be drawn to common tamper notification in BS8243; i.e. there is a restriction that a sequential confirmation cannot occur if a tamper notification is sent from the "activated detector". BS8243:2010 Annex H.1 refers.

Clause 8.8.3 – Monitoring of Interconnections – Table 16 (& Table 17)

a. It must be remembered that the 100s shown in Table 16 is a maximum and the CIE can generate a tamper/ fault signal if a wiring fault/tamper occurs in a shorter timeframe. This is valid for both the set and unset states.

b. The main difference between Tables 16 and table 17 is:
   i. Table 16 – shows the unavailability of interconnections e.g. jamming in a wire-free system.
   ii. Table 17 – shows the verification intervals e.g. polling/supervision.

Clause 8.8.4.1 – Interconnection integrity – Periodic communication

a. For closed loop wiring, interconnection integrity can be provided by the tamper loops in the same cable. This permits the integrity to be checked whilst the alarm contact is open.

b. A fault condition in a 4-wired system is best treated as a tamper to verify an interconnection fault.

Clause 8.8.4.2 Verification during the setting procedure

Use of the term "verification signal or message" in this clause should be understood to mean "periodic communication signal or message" as used in Table 17. This then harmonises with the terminology used in BS EN50131-5-3.

Clause 8.9.1 – Intruder detection, triggering, and the recognition of faults – timing requirements

The following is intended to clarify the meaning of the standard by dividing the timing performance requirements into three phases: Condition developing, recognition and processing.

a. Condition Developing Phase

During this period a component of the system is aware of a potential problem but has not yet determined that it sufficiently constitutes a fault, tamper, hold-up or intrusion. This period is of variable length and determined by the type of condition. For intrusion detection this period shall be the time taken for a detector to signal intrusion*. For fault detection this period is that deemed necessary for the particular fault type (for example: the periods shown in table 16).

***Note**: Example timings are given in the requirements for detectors, for example Clause 4.3.1 of BS EN 50131-2-4.

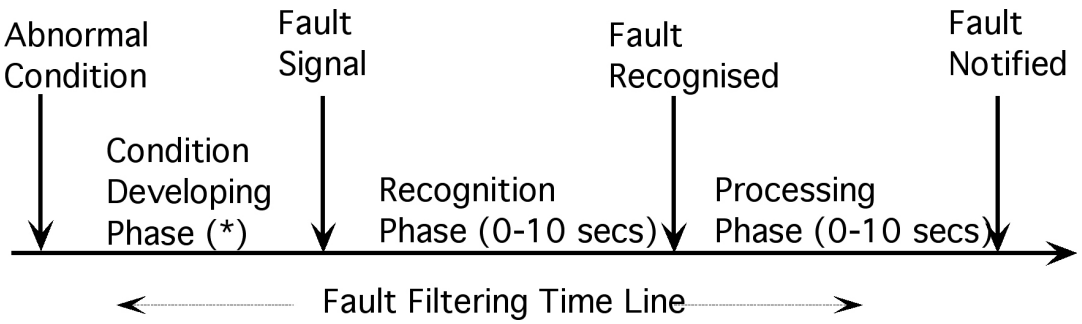
b. Recognition Phase

Intruder, hold-up, and tamper signals with an active period exceeding 400 milliseconds shall be processed. Fault signals present for more than 10 s shall be processed. Signals not exceeding this specified time may be ignored.

c. Processing Phase

This shall be the maximum time permitted to process the recognised fault, tamper, hold-up or intrusion signal and cause any necessary notification, event recording, etc. In all cases this period shall not exceed 10 seconds.

The following time-line uses a fault condition to show the three phases from an abnormal condition occurring until the fault is notified:



= The time period before an abnormal condition becomes a fault condition (the condition developing phase) will vary e.g. see Table 16

Clause 8.10 – Event recording – Table 22

a. In Tables 8, 16 and 22, if an interconnection fault cannot be distinguished from a tamper then it should be treated as a tamper condition (see 8.8.4.1).
b. The requirement for the detector first to alarm in Table 22 may be determined from the order in the event log.
c. The change to site-specific data in table 22 may be a record indicating the change of any or all configuration data. This record is a requirement of DD 263: 2010 Clause 9 c). It is not necessary for the CIE to record a change to each item of data separately. Where the changes are made as part of "remote support" or "remote system checks" in accordance with DD 263: 2010 a full record should be kept of those changes either by the remote "secure computer" or manually. If use is made of a "virtual keypad" then a manual record will most likely be necessary.
d. The term "source" in paragraph 7 needs clarification. It relates to repeated events of the same type from an individual source e.g. multiple fault events from a single detector would result in at least 3 but not more than 10 log events, but a following "tamper" event should be logged additionally in its own right.

This count may be reset in the event of a level 3 restore (see BS EN50131-3) or at reinstatement, as defined in BS 8243:2010

e. If a CIE is used in a lower grade system, the designed-in logging structure does NOT need to be changed to reflect that certain events mandatory at the designed grade are optional at the lower grade.
f. EN50131-3:2009 table 11 and BS 8243: 2010 Annex H.8 identify additional indications that are required.

Clause 9.0 – Power supply

The PSU in the CIE must comply with the requirements of BS EN 50131-6: power supplies. BSIA manufacturers have produced a guidance document for BS EN 50131-6, Form 280 refers.

Clause 9.2 – Requirements

The PPS (or EPS) fault signal permitting reduction of alternative power source requirements in grades 3 and 4 may be sent to a remote centre other than the ARC, provided that this centre is continuously manned and that the PPS (/EPS) fault is included, as a minimum, in a "general fault" signal to the ARC.