bsia
british security industry association

the implementation of **prEN50131-1:2004** – a guide

May 2007

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. 171. Issue 3

Introduction

PD6662:2004 is the foundation document in the UK for the implementation of European Standards for Intruder Alarm Systems – mandatory for all systems installed from 1st October 2005.

Rather than implement the provisions of the published standard, EN50131-1:1997, PD6662 calls up prEN50131-1:2004 – the latest available draft of the revision currently being carried out.

This document has been prepared to give guidance on the interpretation of some of the clauses in PD6662:2004 and prEN50131-1:2004 that have been open to misinterpretation or in need of further clarification. It must be read strictly in the context of the scheme outlined by PD6662:2004. This document may be updated as circumstances require.

Only those items in PD6662:2004 and prEN 50131-1: 2004 which give concerns are listed below. All other clauses or parts of the standard are believed to be self-explanatory.

For simplicity, references in this document to published standards are made as "ENxxxxx" etc. and to Technical Specifications as TSxxxxx, etc.

Whilst prepared initially for use by manufacturers when designing their 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) after consultation with NSI, SSAIB and the insurance industry. The final content has been agreed with those organisations.

This updated issue incorporates:

a) Text changes consequent upon the adoption of product TSs by PD6662:2004 AMD 2.
b) Changes incorporated in the "2006 Industry Statement" but not documented elsewhere.
c) Clarification of certain aspects of "anti-masking" requirements, arising from experience.

Similar guidelines have been / are being made available for each of the available product specifications (TSs) and standards – see below:

These documents do NOT form part of the industry-agreed content of Form 171.

Form 179 MANUFACTURERS' GUIDELINES to the interpretation of DD CLC/TS 50131-3: 2003 Alarm Systems –Intrusion Systems Part 3: Control and Indicating Equipment.

Form 180 MANUFACTURERS' GUIDELINE to the interpretation of BS EN 50131-6:1998 Alarm Systems – Intrusion Systems – Part 6: Power Supplies.

Advisory note:
This guide has been produced for use in PD6662:2004 – Scheme for the application of European standards for Intruder and Hold up alarm systems. With the implementation of PD6662:2010 and the dual running period associated with this transition, other BSIA Industry guidance may have been produced for the later Scheme and therefore you should ensure you seek the appropriate guidance. If you are unsure please contact the BSIA Technical team on 085 389 3889 or email: technical@bsia.co.uk

Interpretation of clauses:

PD6662:2004 Clause 6 (and 4.2) – Documentation

a. It is recommended that the following wording (in addition to any other mandatory requirements) is used in documentation for products to prevent any uncertainty:
   "This product is suitable for use in systems designed to comply with PD 6662:2004 at grade "x" and environmental class" y"."
b. Although not fully in accordance with parts of EN 50136, the following practical approach has been agreed for declaring the performance characteristics of ATS in the UK. The ATE 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.

PD6662:2004 clause C.3.1

This clause includes a requirement for external WDs in all grades to have detection of removal from mounting. This is ADDITIONAL to the requirements of prEN50131-1.

PD6662:2004 clause E.1.1

prEN50131-1 requires an "ATS" fault response, which includes the loss of communication path, and specifies system responses to a loss of ALL intended signalling paths (eg Table 4 note b, Table 5 note b, 8.6 para 6). However, prEN50131-1 Table 1 and this clause of PD6662:2004 require a fault response to be given from a failure of ANY of those paths – though do not require identification of which.

The majority of current equipment does not provide this differentiation; the clause therefore requires the introduction of a new protocol for communication between ATE and CIE.

A standardised agreement for this has been reached between ATE and CIE manufacturers and is available from the BSIA as "Form No. 175 : Manufacturers agreement on the implementation of additional communications requirement between ATE and CIE."

Other methods may be employed.

The clause numbers used from this point refer to prEN50131-1:2004, unless otherwise stated.

Clause 2 – Normative references

EN 50131-6: 1998, including Amendment No 1 - Power Supplies is missing from the list of normative references in prEN50131-1, but is included in PD6662.

Clause 3.1.12 – Alert indication

To clarify, this is the only indication normally permitted at level 1 (see table 9), and 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).

Clause 3.1.42 – Masked

The TS50131-2-x series of detector equipment standards will ultimately define the masking requirements for individual types of detector. In the meantime, movement detectors including a form of masking and meeting the other requirements of PD6662:2004 will be deemed suitable for use.

Clause 3.1.51 – Part set

This definition is felt to be ambiguous and to clarify the meaning the following definition is preferred:
"Status of a zone of an alarm system in which an alarm condition can be notified, but part of the I&HAS is unset"

Clause 7 – Environmental classification

Junction boxes used in all grades of system will need to be environmentally classified, **and declared by the manufacturer to meet the environmental conditions** specified in TS 50131-2-2 (Table 6 and Table 7 refer).

Clause 8.1.3 – Tamper detection

This clause appears to suggest that a tamper signal must be latched to ensure that it is of the minimum duration required by 8.9.1.

The tamper signal referred to is generated once the tamper detector has been activated **for the period required by 8.9.1.**

Clause 8.1.4 – Table 1 Recognition of faults

a. This clause seems to suggest that there is a need to define different faults for the different device types. It is agreed that faults can be derived from the interconnection methods currently available (see pr EN 50131-1:2004 Table 1 NOTE).
b. The term "ATS fault" covers a variety of possible problems, including a "failure to achieve successful connection or to transmit information correctly." This clause does not define how many attempts the I&HAS should make to contact the ARC before declaring a communications fault. 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, this is adopted for all systems signalling to an ARC in the absence of any standards relevant to other ATE currently used for ARC communication.

Clause 8.2.1 – Masking

Detection of masking of movement detectors is mandatory in Grades 3 and 4. It should be noted that Table 1 of TS50131-2-x states that masking may be signalled from the detector as an independent signal, or by signalling "intrusion" and "fault" simultaneously.

Clause 8.3.1 – Table 2 level of access

a. The three asterisks (***) comment appears to apply to the override function only. As there are equally grade dependant factors relevant to the isolate function, the *** comment should be applied to isolation also.
b. The note 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.
c. There are considerable difficulties in understanding the "conceptual" nature of clause 8.3.1 and table 2.
   Attention is drawn to clarification in clause 8.2.1 of TS50131-3:2003.
   (i) Users with level 2 access may additionally be permitted level 3 access specifically to manage level 2 codes as a "master user"; but not to access site specific data. Such users may access this level 3 functionality without further authorisation, and without requiring two separate codes.
   Similarly, a user allocated to level 3 for engineering purposes need not be permitted to access the level 2 code management functionality.
   (ii) prEN50131-1 does NOT require level 2 authorisation for level 3 access to be carried out individually every time such access is required, it may remain in force until manually removed at level 2 – eg permitting an engineer on site to have unlimited access during his visit following a single authorisation.

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) is given. However the second paragraph of this clause additionally permits Level 4 users also to set the system. If this is done, level 2 and 3 authorisation is, of course, required.
b. It is permitted to use a 3-digit code to set for all grades of system.
c. There is no requirement for each user to be individually identified (see table 22), hence having multiple users of the same PIN code (or physical key) is permitted 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 both at transition from unset to starting set and at completion of setting; eg at start and end of exit time, where this is used.
   Note: although not acceptable for DD243 systems, timed setting is permitted by prEN50131-1 and is acceptable for systems not needing to comply with DD243.
c. prEN50131-1 does not specifically require monitoring of the prevention of setting condition throughout the setting period, thus exit strays are allowed as long as all detectors have settled down at the completion of setting. It is recognised that there is a conflict with TS50131-7 (clause 7.3.5.1), which recommends a deviation from exit route to be indicated and prevent the setting procedure from being completed. It is agreed that the TS50131-7 recommendation for prevention of setting be omitted from the PD6662:2004 scheme.
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 8.8.4.1).

Clause 8.3.7 – Set state

There is an apparent conflict between the first paragraph and item (c). In grades 3 and 4, it is not permitted to have an indication showing the set state (clause 8.5.2 - table 9 refers), but a transient indication of the CHANGE of status is mandatory at all grades.

However, as confirmed by table 9, a latched indication of status is permitted for grade 1 and 2 systems, which item c) applies specifically to those systems using a means of unsetting that does not use an entry route. It is therefore implied that this indication would be available before entering the supervised premises and not at the CIE / ACE.

The use of the method of unsetting described at 8.3.7 c) is not considered good practice, and therefore not recommended.

Clause 8.3.8.2 – Unsetting - as specified in clause 8.3.7b

(See Annex A for entry timelines, which clarify this clause)

a. This clause and clause 8.5.2 (Table 9) have been misunderstood, as 8.5.2 does not allow for an alert indication during unsetting. The "alert" does NOT include entry tone functionality. It is agreed that an entry tone is permitted during the entry procedure. If required, the alert will become available when the system is unset.
b. If a user deviates from the entry route during entry time the generation of an alarm condition is not permitted until the expiry of entry time. It is agreed that if a user does this, an audible tone (different from the entry tone) is permitted to inform the user that they have done so. It is recognised that there is a conflict with TS50131-7 (clause 7.3.5.2), which recommends an immediately notified alarm condition. It is agreed that the TS50131-7 recommendation be omitted from the PD6662:2004 scheme.
c. The standard shows that at the end of entry time an alarm condition can be indicated or notified locally, remote notification is delayed for a further 30 seconds. If the system is unset during the 30 seconds then the notification can be cancelled. Refer to figure 2 in Annex A.

Clause 8.3.9 – Restoring

Restore of a condition specified in Table 6 (PD6662:2004 table E.2) 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.

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 fault conditions indicated in table 6 are replaced by Table E.2 in Annex E.3 of PD 6662: 2004.

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 prEN50131-1 and cross referenced in TS 50131-3 CIE clause 8.2.6 and clause 8.2.7.

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 operated in any way and 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 "intrusion," thus Table 7 does not separately itemise responses for this condition.

It is agreed that treating masking as an intrusion achieves all required responses.

NOTES:

a) Provision of the "masking" output from detectors when the IAS is unset is mandatory according to the requirements in TS50131-2-x. This does not allow for the message to be delayed until the point of attempting to set the I&HAS.
b) Provision of the "masking" output from detectors when the IAS is set is NOT mandatory according to the requirements in TS50131-2-x. The only specific system requirement for "masking" is to prevent setting, thus TS50131-2-x does not conflict with prEN50131-1. This has been discussed and agreed between TC79 WG1, WG2 and WG3 in connection with the current revision of these standards.
c) Insurers prefer that the output be used when the system is set, and be processed as an "intrusion" signal. Where this is done, DD243 does not permit intrusion and masking events from the same detector to qualify as a sequentially confirmed alarm.
d) If masking events are to be transmitted to the ARC whilst the I&HAS is unset (eg by inclusion in a "general fault" message), this should be enabled by a specific programming action at the CIE.
e) The detector standards (TS50131-2-x) allow a response time of up to 180 seconds before a detector signals "masking" to the CIE. This is followed by up to 10 seconds permitted for the CIE to process this signal prior to initiating the programmed response. If the signal is to be processed as a "fault"(not the preferred option) then an additional 10 seconds is permitted at the CIE prior to processing.

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. There are three asterisks (***) in the top left hand box of Table 7, their meaning is "signals and/or messages shall be processed according to the status of that part of the I&HAS i.e. set or unset." (TS50131-3 table 9 refers).
d. The table seems to show that system faults and system tampers are to be treated differently. It is unsure 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 differentiation it will be treated as a tamper.
e. In the event of a failure to set what can the system do to alert the user? The standard allows for an alert indication (which may be audible) and/or transmit 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).
f. Table 7 appears to prohibit external WDs operating for a tamper alarm when the IAS is in the unset mode. PD 6662 (C.3.5) allows external WDs to self-actuate in the event of an electrical change to its connections to the control equipment or if its own tamper detection operates.

g. There is some uncertainty over the requirement stated by the two asterisks (**) in the table, as it seems to intimate that an individual detector location would need to be signalled. It must be remembered that aone, as used in prEN50131-1: 2004, is not an individual detector/device. “Zone” is defined as “an assessed area where abnormal conditions 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.
h. 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 DD243:2004 in order to minimise false alarms.

NOTE: replacement Table 7 to clarify these issues is included at page 10.

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

		Grade 1				Grade 2				Grade 3				Grade 4			
*** I&HAS status	Inputs / Outputs	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message
Set	Indication†	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	External WD	Op	M	M	NP	Op	M	M	NP	Op	M	Op	NP	Op	M	Op	NP
	Internal WD	Op	M	M	Op	Op	M	M	Op	Op	M	Op	Op	Op	M	Op	Op
	ATS type messsage	Hold-up	Intruder	Intruder or Tamper	Intruder or Fault $$	** Hold up	Intruder	Intruder or Tamper	Intruder or Fault $$	** Hold up	Intruder	Tamper	Fault	** Hold up	Intruder	Tamper	Fault
Unset	Indication†	NP	M	M	M	NP	M	M	M	NP	M	M	M	NP	M	M	M
	External WD	NP	NP	NP*	NP*	NP	NP	NP*	NP*	NP	NP	NP*	NP*	NP	NP	NP*	NP*
	Internal WD	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP
	ATS type messsage	NP	NP	Op as tamper	Op as fault	NP	NP	Op as tamper	Op as fault	NP	NP	Tamper	Fault	NP	NP	Tamper	Fault

Note: This inclusion in Table 7 of requirements relating to warning devices and alarm transmission systems does not imply that I&HAS must include such devices or systems, however, if such devices or systems are included in an I&HAS they must comply with the requirements of Table 7.

Key: M = Mandatory Op = Optional NP= Not permitted
***** External WD shall not be activated by the CIE in the unset state, but may self-actuate following detection, by the external WD, of WD tamper or loss of interconnection to the CIE.
****** The identity of the Zone of the Hold-Up alarm shall be included in the information transmitted to an ARC
******* Signals and/or messages shall be processed according to the status of that part of the I&HAS. The status of HAS shall be independent of IAS.
† Indications shall comply with clause 8.5 of these requirements, in particular table 9. Only the alert indication shall be available to an access level 1 user
$$ Use of the Intruder signal as allowed by this table is NOT permitted for systems installed to DD243:2004
NOTE: Conditions for "Hold Up signals / messages" whilst Unset refer to the unset status of the HAS part of the I&HAS, where such facility is available.

Clause 8.5.1 – Indications – General

a. In the Note at paragraph 3 of the clause there is an apparent contradiction as it seems to allow for a suppression of an alert indication, yet Table 7 states that indications are mandatory.
   Table 7 does NOT include alert indications and has no bearing on the Note at paragraph 3. The Note does override Table 9.
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.

Clause 8.5.2 – Availability of indications – Table 9

a. Indications permitted by Table 9 are available 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.
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 restored. The term restored in this context does NOT refer to 8.3.9, but means simply that the condition is no longer present. Remember other indications as specified in Table 8 should not be available to an access level 1 user.
b. This requires 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. The requirement specifies that the detector must have means of indication of an alarm condition. Use of this indication at the detector is not mandatory if it is available at the CIE / ACE. Where used, the indication at the detector is restricted in accordance with table 9.
b. Due to the requirements of 8.5.1 and Table 8, all detectors including processing capability must be separately indicated at the CIE at Grade 3 and 4.
   NOTE: PD6662 clause E.6 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. The use of a WD delay with entry deviation and entry timeout alarms is NOT recommended.
c. 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 size of the standby power supply.
d. Where two ATS are specified to meet the requirements of table 10, this should be understood as a standard dual-path system, with the two paths meeting the separate requirements.
e. Communicating devices used only for purposes other than compliance with Table 10 are considered to be non-mandatory equipment and do not affect the security grade of the I&HAS providing they do not interfere with mandatory equipment.
f. The mandatory ATS may additionally carry non-alarm communications providing this does not affect the requirements of EN 50136-1-1 (re: Clause 6.2 of EN 50136-1-1).

Clause 8.7.2 – Tamper detection – Table 12 and Table 13

a. The two asterisks (**) against "Intrusion detectors" in Table 12 refer to the note below the bottom of the table. It is agreed that this note will no longer apply.
b. It is agreed that the note below Table 12 needs clarification. A graded approach is described in TS50131-2-6 which is now a requirement under the PD 6662: 2004 scheme.
c. Table 13 requires Grade 3 and 4 detectors to have a mandatory detection of orientation adjustment. It is agreed that if the orientation of an installed device is fixed and tamper detection of access to the fixing points is provided, then this requirement does not apply.
d. Reference Table 13, note that PD6662:2004, clause C.3.1 adds a requirement for tamper detection of removal from mounting of external WDs at all grades.
e. Table 12 of prEN50131-1:2004 shows that tamper detection of junction boxes is mandatory at grades 2, 3 and 4.
   However, as EN50131-1:2006 will amend this to be mandatory at grades 3 and 4 only, it is agreed that tamper detection of junction boxes at grade 2 should be considered as optional with immediate effect. Good practice recommends the adoption of tampering for junction boxes where they are visible.

Clause 8.7.3 – Monitoring of substitution

It is agreed that in a Grade 4 system all components should be uniquely identified to the system and attempts at substitution detected as specified. Components include detectors, keypads, etc (see table 12) as opposed 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 it is felt that the following apply, as a minimum:

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

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 8.8.5 Security of Communication

The first sentence states that detection of substitution is required at grade 3 and 4 whilst Table 19 says it is mandatory at grade 4 only. The table is correct, as stated in PD 6662: 2004 E.5.

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 TS 50131-2-4.

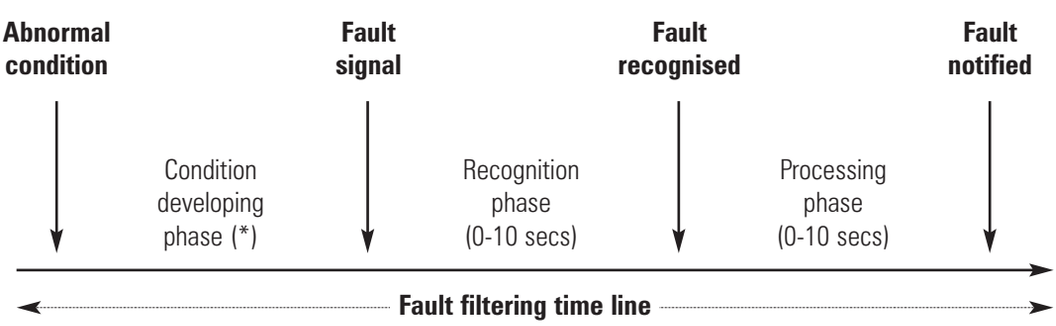
b. Recognition Phase

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 (see the note at the end of Table 22).
c. The change to site-specific data in Table 22 may be a record indicating the change of any or all configuration data. It is not necessary to record a change to each item of data separately.
d. The last sentence of the last paragraph should be a separate paragraph – it is not restricted to grades 3 and 4, as clarified by TS50131-3.
   There is a limit to how many events (maximum of 3) can be recorded from one source (last paragraph of 8.10 refers). TS 50131-3 adds that this should also apply per unset period. (also see DD 243:2004, A.3.1)
e. The term "source" in this paragraph needs clarification. It relates to repeated events of the same type from an individual source. eg 4 fault events from a single detector would result in only 3 log events, but a following "tamper" event should be logged additionally, in its own right. This is clarified by TS50131-3 clause 8.10.5, which also excludes "user actions and soak test events" from this restriction.
f. The first function of Table 22 "User keys when setting" does not mean that every key stroke needs to be logged, just the user identity number associated with the user key as per table 3. This means that it is NOT necessary to identify each user individually – multiple users per PIN code, key, etc. is permissible at all grades, though not good practice.
g. 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.
h. Table 22 does not include the following, which are required by TS 50131-3:2003:
   "CIE Fault" – mandatory for grades 3 / 4 (8.3.3)
   "Input device disabled for code-guessing" – mandatory for grade 4 (Table 3)

Clause 9.0 – Power supply

The PSU in the CIE must comply with the requirements of EN 50131-6: power supplies (also see PD 6662 for clarification). BSIA manufacturers have produced a guidance document for EN 50131-6 that they have accepted.

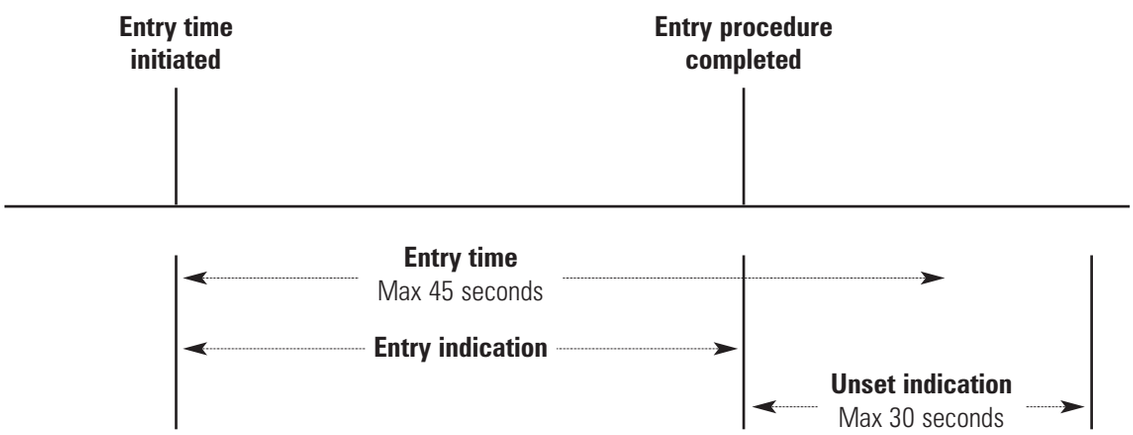
Clause 9.2 – Requirements – Table 23

a. The alternative PSU needs to be able to power the system for the stated period including the operation of all warning devices for 2 alarm periods of up to 15 minutes each.
b. 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 in a "general fault" signal to the ARC.

ANNEX A
Timing diagrams to illustrate operation on entry.

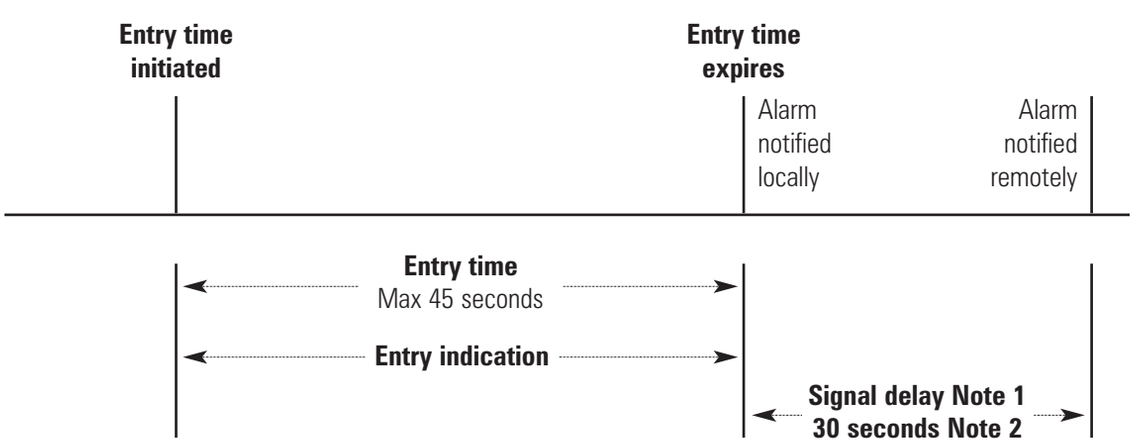
NOTE: The use of WD delay in the case of entry deviation and entry timeout alarms is NOT recommended.

1. NORMAL ENTRY



NOTE 1: Entry indication is not referred to in prEN50131-1.
It is permitted by TS50131-3 (Table 12) and required by TS50131-7 (clause 7.3.4.2).
Indications may be audible.

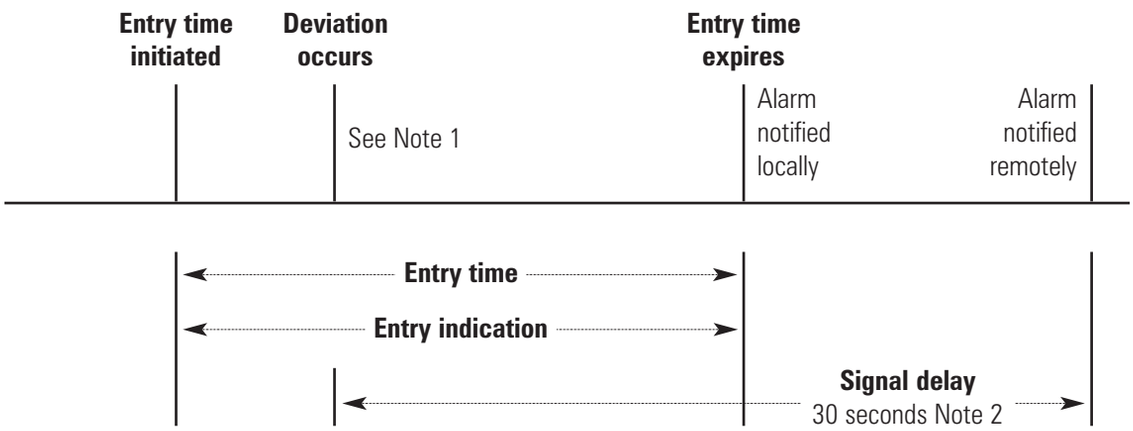
2. ENTRY TIMEOUT



NOTE 1: This signal delay is required by prEN50131-1, but omitted from TS50131-3.
NOTE 2: This delay is cancelled if alarm generated by a detector off the entry route in this period (see DD243:2004).

3. ENTRY DEVIATION – A

Entry Time expires before end of "30 seconds"

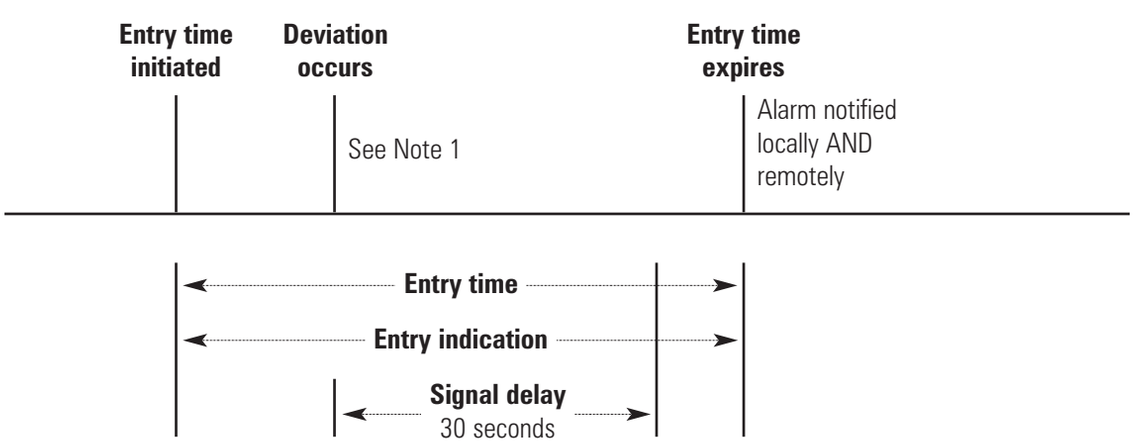


NOTE 1: prEN50131-1 does not permit an alarm to be generated at this point. However, the user must be made aware of the problem in order to correctly unset.
Recommend use of distinctive change to entry tone for this purpose.
NB: TS50131-3 permits the use of internal WD for this purpose

NOTE 2: The "30 second" period is terminated if an additional detector – off the entry route – is triggered after the expiry of entry time (see DD243).

4. ENTRY DEVIATION – 2

"30 seconds" expires before the end of Entry Time.



NOTE 1: prEN50131-1 does not permit an alarm to be generated at this point. However, user must be made aware of the problem to correct unsetting.
Recommend use of distinctive change to entry tone for this purpose.
NB: TS50131-3 permits the use of internal WD for this purpose.