british security industry association

a guide to
DD CLC/TS 50131-3: 2003
part 3: control & indicating equipment

Warning: This guide should be read only in conjunction with I&HAS installed to PD6662:2004 scheme.

June 2012

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

Contents

Introduction

DD CLC/TS 50131-3: Intruder Alarms, Control and Indicating Equipment Requirements has been published. The industry wishes to use this specification as a product standard as quickly as is practical. Unfortunately a problem exists in the UK because DD CLC/TS 50131-3 was written based on the 1997 version of the system standard EN 50131-1. The UK industry has decided to pre-empt the revision of EN 50131-1 by using the latest draft prEN 50131-1: 2004 which has been published by BSI and is called up in PD 6662:2004.

CENELEC is expected to issue EN 50131-3 in late 2006 or 2007. This standard will be based on DD CLC/TS 50131-3 but will take into account the changes included in the next version of EN 50131-1. Until then certain aspects of DD CLC/TS 50131-3 require slight modification, or an interpretation that enable equipment to be manufactured to provide the functionality for systems to comply with the requirements of PD 6662: 2004.

It is intended this guideline can be used by manufacturers to self-certify their products to conform to the technical specification, or be offered to a test house to clarify relevant tests and results.

This guidance document may change as other product specifications (Technical Specifications) are published and adopted in the UK or changes are made to PD 6662.

Only those items in DD CLC/TS 50131-3: 2003 that give concern are listed. All other clauses or parts of the technical specification are believed to be self-explanatory and already in line with the requirements of PD 6662.

These guidelines also comment on the implications of the corresponding specifications for detectors (ie TS50131-2-x series), which impose requirements on the CIE that are not apparent from either prEN50131-1 or DD CLC/TS50131-3.

References

Form 171: BSIA document “Guideline for the use of the PD6662 scheme for the implementation of pr EN50131-1:2004.

Form 180: BSIA Document “Manufacturers’ Guideline to the interpretation of EN50131-6:1998 – Power Supplies”

Form 185: BSIA Document: “Recommendation to Manufacturers for the Interpretation of Detector Standards: – DD TS 50131-2-2, etc.”

These documents are available from the publications section of the BSIA web site www.bsia.co.uk/publications

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

Scope

The TS applies to all components of a system that are used for control and indication. This is not just the CIE, but also ACE. The CIE may be split between two or more housings.

A power supply included as part of, or integrated with, a CIE is subject to the requirements of EN50131-6. Similarly, ATE integrated with CIE is subject to the requirements of the EN50136 series.

Normative references

The TS refers to IK codes. These are specified in EN 62262:2002 – Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code).

Definitions and abbreviations

Clause 3.1.51 Supervised premises

An 'acknowledge' signal emitted by the ARC receiver to the digital communicator to indicate that a transmission of data has been satisfactorily received.

3.1.58 – Unset

This definition is inconsistent with that for "set" at 3.1.45. It should read "status of an alarm system or part thereof." clarifying that it can refer to an HAS or to the HAS part of an I&HAS..

Security grade

To clarify: The CIE and ACE shall meet the requirements of one of four security grades. The security grade of the system that the CIE and ACE are used in is defined by the rules in EN 50131-1.

Functional requirements

Clause 8.1.5 Monitoring (input)

The "Note" refers to EN 50131-5. As yet there is no such document. The original intention was for the EN 50131 standard range to include a part 5 dealing with interconnections by various means. EN 50131-5-3 exists in draft form and may be published in 2005. Other parts in the range 50131-5-X may be created.

8.2.1 and Table 1 – Access Levels

The first paragraph should conclude with a reference to "Table 1".

prEN 50131-1: 2004 uses slightly different definitions for the access levels. The types of user are given as examples only so that in some circumstances Access Level 3 could be, for example, the owner of a system rather than the installer.

Note that clause 8.3.1 and Table 2 of prEN50131-1 are intended to be "conceptual" in nature and are thus difficult to understand. Clause 8.2.1 and Table 1 of TS50131-3 provide a valid interpretation that may be followed.

See also Form 171 (clause 8.3.1 c).

8.2.2 Authorisation

a) The required number of physical key differs are greater for grades 2 and 3 in prEN 50131-1: 2004. Despite the apparent anomaly at grade 2 of the physical differs being greater than the logical differs, the requirements of prEN 50131-1: 2004 should be used. That is 15,000 differs at grade 2 and 30,000 at grade 3.

Note: Clause 8.3.4 of pr EN 50131-1: 2004 permits setting of the system to be performed by codes equivalent to those of grade 1.

b) Where the code is not confirmed by the user, and the CIE continually checks the most recently entered digits for codes, the number of incorrect entries should be calculated by to the number of key presses, according to the formula:

$$\text{Number of incorrect codes} = \frac{\text{number of key presses}}{\text{number of digits in code}}$$

8.2.3 Setting procedure and 8.2.4 Unsetting procedure

Note that these functions are not mandatory for HAS, or HAS parts of I&HAS (see prEN50131-1, 8.3.3).

8.2.3.1 and 8.2.3.2 Prevention of Setting

Tables 4 and 5 of the TS also appear in a slightly modified way in prEN 50131-1: 2004 as tables 4 and respectively. The prEN 50131-1 versions of the tables should be used.

8.2.4 Unsetting Procedure

The mandatory requirement to include a means of unsetting applies to the IAS. Clause 8.3.3 of prEN 50131-1: 2004, together with the definition of unset, clarifies that it is not mandatory to provide an unsetting facility for HAS.

8.2.4.3 and 8.2.4.4 Unsetting

The various documents contain conflicting requirements regarding the use of an entry route during unsetting. It is recommended that the solution stated in "BSIA Form No 171" (Clause 8.3.8.2) should be used.

The Note following paragraph 2 of 8.2.4.3 is explanatory only and refers to false alarm reduction. The reference to EN 50131-1 Clause 8.3.3.3 is to the 1997 version. That clause is now 8.3.8.2.

8.2.5 Table 6 – Authorisation to restore

This table differs from that of EN 50131-1 and PD 6662. For the UK the Table E.2 in Annex E of PD 6662: 2004 should be applied.however does permit this. Refer also to "BSIA Form No 171,", Clause 8.3.12.

8.2.6 Inhibit Function

The use of the term "inhibit" in this clause is inconsistent with the definition of 3.1.26. For example inhibit of user interface does not simply mean that the user interface cannot generate an alarm. If there is doubt the word should be taken to mean: "disabling of a function".

Note that the optional (OP) automatic inhibit of "User Interface" in table 7 does not mean that the mandatory requirements at grade 3 and 4 in Table 3 (8.2.2) can be ignored.

The reference to "Authorisation Codes" in table 7 is not understood, but is not mandatory.

prEN 50131-1: 2004 Clause 8.3.10 does not indicate that access level 3 users may inhibit. Table 8 of TS 50131-3 is more sensible and should be applied with the following exception.

prEN 50131-1: 2004 Clause 8.3.12 requires that a test facility for hold-up devices should be available to access level 2 users. Table 8 appears to imply that this test cannot also inhibit the hold-up signals. The definition of test however does permit this. Refer also to "BSIA Form No 171,", Clause 8.3.12.

To avoid confusion the reference to Table 15 of EN 50131-1: 1997 should now refer to Table 22 of prEn50131-1:2004.

8.2.7 Isolate operation

To avoid confusion the reference to clause 8.3.7 of EN 50131-1: 1997 should now refer to clause 8.3.11 of prEn50131-1:2004.

8.2.9 Other functions

Clause 8.3.13 of prEN 50131-1: 2004 takes precedence. This permits access level 3 users to perform operations that adversely affect the system (for example, during test).

8.3 Processing

To avoid confusion the reference to Tables 3, 4 and 5 of EN 50131-1: 1997 should now refer to Tables 7, 8, 9 and 10 of the 2004 draft. However care should be taken, because the tables have been modified between the two versions and cannot be used without further interpretation. This is included below, see comments regarding "Table 9", "Tables 11 and 12" and "Clause 8.5 and Table 13" in this document.

Table 9

Table 9 of TS 50131-3 is superseded by Table 7 in prEN 50131-1: 2004. However that table contains errors and does not include provision for self-actuation of external warning devices. A revised table has been proposed for inclusion in a new draft of EN 50131-1 and this may be used instead. A copy of this table (with notes, etc. adjusted to correspond with TS50131-3 references) can be seen on page 6.

8.3.1.1 Alarm Inputs

This clause should be read to say:

"Intrusion alarm signals shall be processed. This may be done individually to generate one or more intruder alarm conditions. Alternatively, an alarm condition may be generated by the logical combination of signals or messages within a defined time window from the same alarm point, or from logically grouped alarm points."

Note that DD243 affects the operation of a system with regard to this clause.

8.3.3 Monitoring of Processing

This clause places requirements upon CIE design that restrict development whilst at the same time do not monitor likely causes of failure.

It is suggested that the following requirements are used instead (changes are in italics):

a) The processing monitoring function shall respond to a complete failure of the processing function.

b) for a grade 4 CIE, an output shall be provided which shall change state when the processing monitoring function activates, this output remaining until manually reset;

c) for grades 3 & 4, the operation of the processing monitoring function shall attempt to restart the processing

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

*** I&HAS status	Inputs / Outputs	Grade 1				Grade 2				Grade 3				Grade 4			
		Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message	Hold-up signal/ message	Intruder signal/ message	Tamper signal/ message	Fault signal/ message
Set	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 message type	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 message type	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: The inclusion in thisTable 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 this Table.

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 and (in particular) table 9 of prEN50131-1:2004. 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 (this note was not included by BSI for submission to CENELEC).

and generate a CIE fault signal or message, this event shall be logged and indicated;

d) when the processing restarts, as required by c) above, the I&HAS shall resume operation in its previous operating mode (EXAMPLE: set or unset).

See also the associated test in 12.4.9

8.4.1 Indication

Paragraph 3 describes what prEN 50131-1: 2004 calls an 'alert' indication. This is not optional, it is a mandatory requirement (see prEN50131-1 table 9).

Paragraph 2 describes what prEN 50131-1: 2004 calls a 'pending' indication.

8.4.1.1 and 8.4.1.2 Alarm, tamper, fault and other condition indications

The indications available at any time should follow the requirements of prEN 50131-1: 2004. Refer to "BSIA Form No 171", Clause 8.5.3.

In addition the term "individual acknowledgment" may refer to individual by type rather than source. For example: The triggering of three hold-up alarms and a low-battery warning would then require one acknowledgment for the hold-ups and one for the low-battery.

Although the standard appears to state that every individual alarm indication (and hence every detection) requires separate acknowledgement, the UK considers this cumbersome and prefers "acknowledgment by type".

To briefly clarify the requirements of prEN 50131-1: 2004 (including those affecting TS 50131-3 Clause 8.4.1):

- An alarm, tamper, or fault condition shall create the need for an "alert" indication. This may be visual and/or audible. Acknowledgment of the condition while it is still present may change the nature of the "alert" indication (e.g. by stopping a warning sound, or converting a flashing visual display to continuous, etc).
- A user at access level 2 may view the detailed information relating to the alert and, when more information is available than can be shown, a "pending" indication is required. The detailed information should be hidden from non-authorised users, for example by removal following a time delay. This adjusts Clause 8.4.1.2.
- The "alert" indication should remain until the condition causing it has been removed and the user has subsequently acknowledged the condition.

Tables 11 and 12

Tables 11 and 12 are based on the indication requirements of EN 50131-1: 1997. The impact of the changes described above (re: Clauses 8.4.1.1 and 8.4.1.2) makes these tables overly complicated. In some cases there are conflicts between the tables and prEN 50131-1: 2004. The lists of "conditions to be indicated" are however useful and it should be mandatory to show some of these conditions to a user attempting to set the system. These requirements can be summarised by the two tables below which is based on an amalgamation of the requirements of both prEN 50131-1: 2004 and TS 50131-3.

It is recognised that in some cases the action of attempting to view a condition might have a side effect of changing it. For example, if a system is set, use of a proximity tag to view the state may in fact unset it.

11A - Indications at Access Level 1

Conditions to be indicated	Grade			
	1	2	3	4
Set / Part Set/ Unset State	OP	OP	NP	NP
Setting Complete (“Transitory”)	M	M	M	M
Unsetting Complete (30s Max.)	M	M	M	M
Entry/Exit Indication	M	M	M	M
Alert Indication	M	M	M	M

NP = Not Permitted, Op = Optional, M = Mandatory

* The requirement applies only if the cause of the indication is included by the system or equipment (e.g. Entry/Exit indication is only required when a system includes an entry or exit route).

11B - Indications at Access Level 2

Conditions to be indicated*	Grade				Shown at setting **
	1	2	3	4	
Set / Part Set/ Unset State	M	M	M	M	M
Intruder Alarm	M	M	M	M	M†
Hold-up Alarm	M	M	M	M	M†
Tamper Alarm	M	M	M	M	M†
Zone of Intruder or Hold-up Alarm (NB Zone, not Alarm Point)	M	M	M	M	Op†
Alarm Point causing Alarm	Op	M	M	M	Op†
Alarm Point First-to-Alarm	Op	M	M	M	Op†
Alarm Point Isolated	Op	M	M	M	M
Alarm Point Inhibited	Op	M	M	M	M
Alarm Point being soak tested	Op	M	M	M	M
General Fault	M	M	M	M	M
PPS (Prime Power) Fault	M	M	M	M	M
APS (Auxiliary Power) Fault	M	M	M	M	M
ATS Fault	M	M	M	M	M
Detector Masked	Op	Op	M	M	M
Range Reduction	Op	Op	Op	M	M
Failure of processing	Op	Op	M	M	M†
Interconnection Fault	Op	M	M	M	M
Power Output Fault	Op	Op	M	M	M
Pending Indication	M	M	M	M	M

NP = Not Permitted, Op = Optional, M = Mandatory, N/A = Not Applicable

* The requirement applies only if the cause of the indication is included by the system or equipment (e.g. Hold-up alarm indication is only required when a system includes a hold-up alarm).

** The indication shall be shown to an access level 2 user when the condition requires, or is the result of, an override (see 8.2.3.2) in order to allow setting or if the condition reduces the performance of the I&HAS (e.g. soak test). It is mandatory to show the indication during setting only if the indication is shown as mandatory for the grade.

†The ability to set the system whilst a restore is required is not normal usage in the UK. It is possible that the user action to set the system causes the indication to be displayed and then permits restore at the start of the setting procedure.

8.4.3 Setting/Unsetting Indication

Some of the stated time restrictions conflict with prEN 50131-1: 2004. Indication of completion of unsetting is limited to 30s maximum. Indication at the point of entry of set or unset state at grades 1 and 2 are unrestricted (re: Table 9 of prEN 50131-1: 2004). Clause 8.3.7 of prEN 50131-1: 2004 permits the indication of completion of setting to be “of sufficient duration to enable a user to ascertain the status of the I&HAS.”

For assistance in understanding this issue, the following interprets the requirements of prEN 50131-1: 2004 (all references are to that document):

> Table 9 says that at grades 1 and 2 it is permitted to show the “set status” of a system. This agrees with 8.3.7 c) (which is also limited to grades 1 and 2).
>
> Clause 8.3.7 paragraph 1 uses the term “transitory indication”. This indication is not an indication of the set status; it is an indication that “the system…has changed to a set state”. In some cases this could be the same indication but the “transitory indication” is mandatory in all grades and is therefore not the same indication referred to in 8.3.7 c) or Table 9.

8.5 and Table 13 Notification Outputs

Table 10 of prEN 50131-1: 2004 as amended by Annex E1.2 of PD 6662: 2004 should be used instead of table 13. Note that the shaded areas are optional (not “Not Permitted”).

It is permitted to suppress the operation of Warning Devices as specified in Clause 8.6 of prEN 50131-1: 2004, for example during a hold-up alarm.

8.6.2

To clarify the requirement of paragraph 3: Whilst opening a mounted CIE or ACE by “normal means”:

> At grade 1 and 2 it should not be possible to introduce a tool of 2.5mm diameter without operating the tamper devices. The test does not include the normal openings around switches, displays, etc that appear whilst opening.
>
> At grade 3 and 4 it should not be possible to introduce a tool of 1.0mm diameter without operating the tamper devices. The test includes all openings but excludes damaging the equipment (that is covered by “penetration”).

8.6.2.2 Penetration of the Housing

Further clarification is required.

8.7 and Table 18 Faults

“CIE Fault” and “Monitoring of Processing” are synonymous and should only appear once in the table (re: clause 8.3.3).

The inclusion of “other components” means that if any component not listed elsewhere in the table is included in a system then the CIE shall be capable of receiving a fault signal from it. For the purposes of satisfying this requirement it is not necessary to provide individual identification of the component nor is there any stated requirement that this fault condition causes a particular response. Only the faults listed as Mandatory in Table 1 of prEN 50131-1: 2004 have defined responses.

The note (*) about “primary cells” in fact applies to any storage device used for a type ‘C’ power supply.

Table 18 refers to “Prime power fault”. Depending on the type of power supply this may be indistinguishable to the CIE from “EPS” or “Battery change required”. For further information on power supply terminology refer to BSIA Form 180.

It is not necessary to recognise faults listed in the table that are not applicable. For example “EPS” does not apply to a battery driven CIE and “ATS fault” does not apply to equipment without signalling capability.

8.9.5 (and other parts of 8.9) Timing

Clause 8.9.5 conflicts with the timing requirements of prEN 50131-1: 2004. The 10s allowed for notification commences after the completion of the times stated in 8.9.1 to 8.9.4 inclusive. This is clarified by the diagram included with the commentary on Clause 8.9.1 in “BSIA Form No 171”.

8.10.4 Retention Following Power Failure

This does not apply to grade 1 CIE (Refer to Table 21 of prEN 50131-1: 2004).

8.10.5 Number of events from a single source

During each set period and each unset period no more than three alarm occurrences should be recorded from a single source. The count is reset when the system is set and unset. To facilitate correct diagnosis of false alarms from DD243 compliant installations the count of events from the same source shall be cleared following re-instatement at the end of the confirmation time. Refer to DD243: 2004 Clause A.3.1 for further information.

8.10.6 Permanent Record Facility

In the “NOTE” the phrase “means to operate an appropriate external device” should be taken to read “means to transfer the event log to an appropriate external device”. It is not necessary for the CIE to control the external device.

8.10.7 Event Recording at the ARC or other remote location

The requirements for “temporary memory” apply to both the number of events and the endurance of recording given in Table 21 (not Table 14) of prEN 50131-1: 2004.

Product Documentation

Clause 10 does not list all of the necessary items for inclusion in the documentation. The following items (see chart on page 11) are missing from the list but are included elsewhere in TS 50131-3

Additionally the testing (e.g. 12.4.4) specifically states that the manufacturer must specify the tool(s) required for normal access to the CIE and ACE.

Documented Item:	**Stated in Clause:**
Security Functions additional to those in table 1	8.2.1 and 8.2.9
Sub-level allocations of functions in table 1	8.2.1 and 8.3.2
Non Security Functions	8.2.1 and 8.2.9
Number of invalid code entries before user interface disabled	(not included in 8.2.2,probably should be)
Inhibit of functions (not covered by "n" and "m")	8.2.6
Criteria for automatic removal of soak test attribute	8.2.8
Priority of signal and message processing	8.3.1.2
Priority of indications	8.4.5
Available Notification Options of Table 13	8.5
Type of Interconnections	8.8.1
Type of CIE or ACE (Fixed, Movable, Portable)	13.1

Tests

Optional features that are not provided by the equipment under test do not have to be tested.

Clause 12.1.3

The requirements for the quantity of equipment to be tested are excessive whilst at the same time not rigorous. The following alternative to 12.1.3 b) is considered better:

- The greater of one or 10% of the maximum system capacity of each type of ACE and expansion device shall be tested (e.g. if a system can have 20 proximity readers, 10 keypads, and 30 expansion modules, then test at least 2,1 and 3 of each respectively).
- For the CIE each ACE and expansion device the greater of 5, or 10% of the maximum capacity of alarm points that can be directly connected or (for wire-free) programmed to that device shall be connected.
- For wire-free equipment at least 8 wire-free alarm points shall be tested.
- If any of the above determinations result in a number greater than the capacity of the device or system the maximum number possible shall be used instead.
- When connections to the CIE are by the use of multiple bus systems, or by wire-free and wired interconnections, the alarm points shall be evenly distributed across the connecting media.

Note: Typically this could result in a 100 alarm point capacity CIE being tested with 34 alarm points instead of the 100 stated in the TS.

12.1.4 – Power Supply

The phrase "at least at" (in the final sentence) should say "at a level of at least".

12 - Tables 20, 21, 22, 23 and 25

The references to clause 8.8 within the tables are incorrect and can be ignored.

The pass/fail criteria have been written with respect to EN 50131-1: 1997. The indications are now different and should meet the requirements described in the section of this document headed "Tables 11 and 12". Whenever tables 11 and 12 or Clause 8.4 or 8.4.1.1 are mentioned in the tables the revised table 11 given in this document should be used.

The places affected are:

Table 20: Steps 2, 3 and 5

Table 21: The "General Criteria" and Steps 2 and 8

Table 22: The "General Criteria" and Steps 2 and 8

Table 23: The "General Criteria" and Steps 2 and 8

Table 25: The "General Criteria" and Steps 2 and 8

Whenever Clause 8.2.5 is mentioned in the pass/fail criteria the response should be not as clause 8.2.5 but instead as per Table E.2 of PD 6662: 2004. The places affected are:

Table 21: Steps 3 and 9

Table 22: Steps 3 and 9

Table 23: Steps 3 and 9

Table 25: Steps 3 and 9

12.4.1 Table 21 – Intruder Signal Tests

Step 1. The maximum permitted time for recognition and processing of an intruder signal is 10.4s, not 10s as stated in the pass/fail criteria.

Step 5. This step is superfluous because it is repeated four times in step 6.

Step 6. It is not necessary to repeat step 3 as part of step 6 because the CIE should not require a "restore".

12.4.2 Table 22 – Hold-up Signal Tests

References to "set and "unset" in this clause refer to the status of the HAS, not the IAS. It is not mandatory to provide a facility to unset the HAS and so the related tests may not be needed.

Step 1. The maximum permitted time for recognition and processing of a hold-up signal is 10.4s, not 10s as stated in the pass/fail criteria.

Step 5. This step is superfluous because it is repeated four times in step 6.

Step 6. The word "intruder" in the test condition should read "hold-up". It is not necessary to repeat step 3 as part of step 6 because the CIE should not require a "restore".

12.4.3 Table 23 – Tamper Signal Tests

References to "set and "unset" in this clause refer to the status of the HAS, not the IAS. It is not mandatory to provide a facility to unset the HAS and so the related tests may not be needed.

Step 1. The maximum permitted time for recognition and processing of a hold-up signal is 10.4s, not 10s as stated in the pass/fail criteria.

Step 2. The word "intruder" in the test condition should read "tamper". It is not necessary to repeat step 3 as part of step 6 because the CIE should not require a "restore".

Step 5. This step is superfluous because it is repeated four times in step 6.

Step 6. A tamper applied in the unset state should cause an tamper condition. The note in step 6 should therefore be the same as the note in step 4 and the pass/fail criteria should also be the same as step 4.

12.4.4 and 12.4.6

These clauses refer to an "appropriate tool". This is a tool specified by the manufacturer to obtain access to the internal components of the CIE or ACE (see Clause 10).

12.4.5 - Tamper Protection (impact)

The test procedure in d) refers to grade dependencies. Clause 8.6.1 contains the requirements but there are no grade dependencies. The test should therefore not include the indicators and operating controls.

12.4.6 - Tamper Detection

To avoid confusion about the equipment, replace the second part of the test procedure in d) with:

"Whilst opening, attempt to introduce a test probe into the housing. For grades 1 and 2 the test probe shall be the test rod as specified in EN 60529 Table VI. For grades 3 and 4 the test wire of EN 60529 Table VI shall be used."

12.4.8 - Penetration

To carry out the test exhaustively it would be necessary to make several holes. Depending on the method of detection used it may be necessary to block a previous test hole or replace the housing before a further attempt. The manufacturer should advise the test house what is necessary.

Note that the test cannot produce a guaranteed result unless every possible hole location is tested without failure to detect a tamper. This is unreasonable. It is expected that a test house will analyse the design for the potential weakest point.

Holes only need to be created through surfaces exposed when mounted.

The tamper detection should be operational in both set and unset states (re: prEN 50131-1: 2004 Clause 8.7.2) and therefore the test need only be performed in one state.

12.4.9 – Process Monitoring

With reference to clause 8.3.3 c) the requirement is only to "attempt to restart". It is not possible to detect a failed attempt. No other requirements exist at grade 3 therefore this test only applies to grade 4.

12.4.10 Table 25 – Fault Signal Tests

Step 1. The maximum permitted time for recognition and processing of a fault signal is 20s, not 10s as stated in the pass/fail criteria. Certain conditions may not be recognised within this time (e.g. telephone line fault).

Step 7. Systems may not be capable of generating the number of faults specified. In this case as many faults as possible should be generated.

12.4.11 – Processing

The title should say: “not specified” instead of “non specified”.

12.5.1 – Access Levels

For the tests to match the requirements of PD 6662 the references in Table 27 should be changed. Instead of Table 5 of TS 50131-3 refer to Table 5 of prEN 50131-1: 2004. Instead of Table 6 refer to Table E.2 of PD 6662: 2004.

12.6.4 Table 30 – Test of Setting Procedure

The pass/fail criteria of step 1 should read: “The setting procedure shall be prevented in accordance with Table 4 and 8.2.3.”

In all cases the prEN 50131-1:2004 versions of the table 4 should be used.

For the tests involving overriding the pass/fail criteria should refer to table 5 when necessary (using table 5 of prEN 50131-1:2004). The tests are only valid if optional inhibition and overriding is possible.

12.6.6– Entry and Exit Route

Table 32

The operation of internal warning devices and timings should correspond to the method described in BSIA Form 171

In step “unsetting is proceeding” the 30s referred to is a minimum figure. If the manufacturer has implemented a longer time they should inform the test house.

Table 33

The second set of test conditions beginning “CIE unset” are superfluous duplicates and can be ignored.

12.6.7 Table 34 – Event Log

Step B is optional. Cyclic methods of storage are not mandatory. If the manufacturer employs a storage method that will not pass this test they should inform the test house.

Step F is unnecessary if the equipment uses non-volatile storage (e.g. EEPROM). The manufacturer should instead supply the test house with the component manufacturer’s data for the memory devices used, highlighting the data retention periods.

Step M. The accuracy of the clock should be measured and any error should equate to less than 50s in 30 days. An additional 10s is permitted if measuring from the event log. (re: clause 8.10). For example, a test performed over 9 days should have an error of less than 25s.

Environmental tests

13.2 Table 35 – Environmental test selection

Only the tests specified are mandatory. Other tests in EN 50130-5 are not required.

Annex A

A.1 to A.3: The terms are better explained by the definitions of prEN 50131-1: 2004 Clauses 3.1.46, 3.1.63 and 3.1.84.

Annex B

If Portable ACE is used to meet the requirements of Clause 8.2.2 then PIN codes of fewer differs must be discounted for the purposes of this calculation.

See also comment b) on 8.2.2.

Annex C

The column marked "notify within" means that after processing the notification should occur within the time stated. For example the intruder alarm notification should occur within 10.4s of the start of the intruder signal.

There is no reference to a "memory integrity check" within the standard. This may be ignored.

The "main program watch-dog" time should state 10s (re: Clause 8.3.3 a) and test 12.4.9).

For EPS fault: The reference to clause 8.3.1 should refer to clause 8.5. The "1h" in the column "process if more" is incorrect. It is the notification that may be delayed by one hour, processing should occur if it lasts more than 10s.

Additional Recommendations

DD CLC/TS50131-2-x series - Requirements for detectors

General

The TS 50131-2-X specifications include requirements for a number of signals or messages to be sent between the CIE and detectors and methods of doing so.

prEN50131-1 and TS 50131-3 do not include all of these details.

The requirements – and potential requirements – affecting CIE are summarised below, with recommendations on how they should be dealt with at the CIE.

NOTE: unless otherwise stated, clause and table references are to TS50131-2-2 – the provisions of other TSs are similar, where the function is relevant to the detector type.

A.1. Signals/Messages from Detectors

A.1.1 Signals up to grade 3

There are requirements for the following signals to be sent by the detector to the CIE:

Intrusion	
Tamper	
Fault	(Optional at grades1 & 2)
Masking	(Optional at grades 1 & 2)

Table 1 of TS 50131-2-X includes details of a matrix of the intrusion, tamper and fault signals to be used to indicate masking detection, as well as separately identifying power problems and self-test results.

The provision of an optional dedicated “masking output” is permitted.

At grade 3 (and grades 1 and 2 if optional features are used), this “matrix” is the preferred method of interconnection, permitting fewer interconnection cores to be used and simpler implementation for the installer.

The matrix appears as Table 1 of TS50131-2-x and has been clarified in BSIA Form 185.

NOTE: Use of a “common” fault or masking connection for multiple detectors does not permit the system requirements of prEN50131-1 to be fully met.

The table permits other conditions to result in an incorrect “masking” response at the CIE. Therefore, outputs from detectors should be prioritised such that “fault” and “intrusion” signals will be combined only for a “masking” event.

A.1.2 Signals at grade 4.

In addition to the above signals, there is a mandatory requirement for a “reduction of range” signal. The table does NOT include reference to how this signal should be communicated.

At grade 4, “bus”-based systems are expected to be the normal method of interconnection.

A.2. Signals/Messages from CIE to Detectors

A.2.1 Detector Alert (set) / Standby (unset) mode

TS50131-2-X, clause 4.1 includes the requirement:

“All detectors shall have an alert/set mode. Grade 3 and 4 shall have an unset (ie stand-by) mode”.

Although this is a mandatory requirement for detectors, there are no mandatory functional changes resulting. The relevant optional feature is the ability to disable the “masking” output when the IAS is set.

If this facility is required, it would appear that the standard IAS “SET / UNSET” configuration will suffice.

NOTE: The UK insurance industry has expressed a preference for masking to give an “intrusion” response whilst the IAS is set.

A.2.2 Detector "intrusion" enable

Table 1 of TS50131-2-X states that the intrusion signal is "not required in unset/standby mode – required in test mode."

If implemented in this way, it would prevent the IAS from giving the correct "prevention of setting" response and would therefore need the detector output to be specially enabled by the CIE as part of exit procedures in order to comply with prEN50131-1.

Detectors are expected to standardise with the intrusion signal remaining available whilst in "standby" mode, but some situations (eg those associated with the use of wire-free detectors) may require the permitted functionality to be provided.

NOTE: In the event of a detector functioning in this way, it would be necessary for the CIE to provide this output also when the "Walk Test" function is required (at access level 2 and 3) to enable the "intrusion" signal to be live during testing.

A.2.3 Detector Indication Enable

TS50131-2-X, Clause 4.2.2 states that:

"An indicator, if provided at the detector, shall indicate when detection causes an intrusion signal or message. This indicator shall be capable of being enabled/disabled. This operation shall only be performed locally after removal of the cover or remotely at the control and indicating equipment."

Authorisation to view such indicators is governed by prEN50131-1 table 9.

Contrary to the impression given at 4.1, this indication enable cannot be controlled by the "alert/standby" mode of the detector.

A special "indication enable" signal may therefore be required from the CIE – live during "Walk Tests" and when level 2 access is obtained following the generation of an "alert" condition – or restrict the enable to be performed locally only, as permitted.

As the use of multiple detectors covered by a single indication at the CIE is likely to be extremely rare, it is probable that "local" enable of the indication at the detector for engineering test purposes will be sufficient for general requirements.

A.2.4 Detector Remote self-test

Clause 4.3.5 of TS50131-2-X identifies a "self-test" of the detector, which may EITHER be performed automatically OR initiated remotely.

Detector manufacturers have agreed that the automatic self-test can be considered as mandatory and will be conducted at least once every 24 hours. This (along with supply problems, etc.) will provide the stimulus for the "fault" signal required by prEN50131-1.

The remotely initiated self test is optional, and (if available) may be required to be used in some remote maintenance applications.

If the remote self-test is used, the detector responses will be as per Table 1. The detector response will be received within 10 seconds, but a further 5 seconds are permitted for detectors to return to normal operation.

Detector manufacturers are expected to "randomise" the test to minimise current surge demands from the system PSU, etc.

NOTE: the "remote self test pass" signal will typically be active for 2.5 seconds.

During a remotely initiated detector self-test, it will be necessary for the CIE to distinguish between detectors which are expected to return a "pass" message and those which are not (eg door contacts), perhaps by use of an "alarm point attribute."

As a significant number of detectors could be signalling near-simultaneously, it may be necessary to group the detectors and test these groups separately, using a series of outputs from the CIE sequentially to initiate this.

A.3 Power Up Initialisation

TS50131-2-X, Clause 4.3.2 permits:

"The detector shall meet all functional requirements within 180s of the power supply reaching its nominal voltage."

The implication of this is that the CIE may need configuration to allow responses from detectors to be ignored, and setting prevented, for a certain period after power is applied. This is not expected to be a problem for detectors for which the TS50131-2-x series is currently applicable, but there may be a future requirement to take this into account – especially during the setting procedure - for detectors that use a "power-down" reset.

A.4. Summary

The following table summarises all of the actual or potential signals and messages at each grade:

Signal or Message	Source	Grade				For detail, see reference to:
		1	2	3	4	
Detection (intrusion)	Det.	M	M	M	M	As matrix: see A.1.1 and Table A.1
Tamper	Det.	M	M	M	M	
Fault	Det.	Op	Op	M	M	
Masking detected	Det.	Op	Op	M	M	
Range Reduction detected	Det.	Op	Op	Op	M	A.1.2
Alert/Set – Standby/Unset	CIE	Op	Op	P	P	A.2.1
Intrusion enable	CIE	P	P	P	P	A.2.2
Indication Enable	CIE	P	P	P	P	A.2.3
Remote Self Test	CIE	Op	Op	P	P	A.2.4
Power	PSU	As required by detector				
Det = Detector, M = Mandatory, Op = Optional, P = Potential requirement						
Note: "P" is used to differentiate an action that may be required at that grade (dependant upon detector and system design) from one that is purely optional for that grade.						

Document history

Date	Issue	Comment
30/04/05	Issue 1	First issue
30/06/05	Issue 2	Multiple changes to harmonise with other European standards
23/06/12	Issue 2.1	Reconfirmation of 5yr review. Retained for use in I&HAS installed installed to PD6662:2004