# ALL YOU NEED TO KNOW ABOUT THE

# NEW STANDARDS

## IN ONE HANDY POCKET GUIDE

Updated for 2016 to include IA1501

Brought to you by:

CSL

In association with:

NSI Security.Improved

SSAIB

This Pocket Guide has been designed as a quick reference to key changes to the standards. For a full explanation of any points referenced please consult the full standards or contact your Certification Body.

## WHY DO WE NEED THE INDUSTRY AGREEMENT?

The 2015 PD 6662 update has been delayed. A temporary arrangement has been adopted by the industry in the form of the Industry Agreement – IA1501.

## REMOTE DEVICES FOR SETTING/UNSETTING

For all IAS, completion of full setting must be possible by one of the methods listed in Clause 6.3 of BS 8243. This must be the configured default method of setting. It is not permitted to use a timed setting procedure when setting is performed on site. In addition, setting of the IAS can be achieved by use of a device as a non-I&HAS interface taking into account the following:
The requirements of Annex C of EN 50131-3 must be met except that 8.7.3 (Monitoring of Substitution) and 8.8 (Security of Communication) apply to Grade 4 systems only.
For all systems setting is permitted only if the requirements of BS EN 50131-1 Clause 8.3.5 "Prevention of setting" are met.
The timed setting procedure (min 30 seconds, max 60 seconds) must include an audible indication throughout the supervised premises and the procedure must be cancelled if any intrusion detector is in active condition.
Confirmation of whether the IAS has set, failed to set, or that an error has occurred must be provided to the user by the remote device on the basis of information sent to it by the CIE.
(IA1501 4.1)
For all IAS, unsetting must be possible by one of the methods listed in Clause 6.4 of BS 8243. This must be the configured default method of unsetting. In addition it is permitted for unsetting of the IAS to be achieved by use of a remote device.
(IA1501 4.2)

## EVENT RECORD

The CIE event record must hold all instructions to unset and initiate setting and include identification of the user or the remote device
(IA1501 4.3)

## SYSTEMS

The system design proposal and as-fitted document must state that the I&HAS conforms to PD 6662: 2010 + IA 1501: 2015 at the security grade and notification option applicable to the system
(IA1501 5.1)

## COMPONENTS AND CABLES

Components conforming to BS 4737-3.10: 1978 or PD CLC/TS 50131-2-8:2012 are permitted (Shock sensors).
When cable is installed by the alarm company (including sub-contractors), it must conform to BS 4737-3.30: 2015.
When existing systems are upgraded, cable conforming to BS 4737-3.30: 2015 must be used on the new part of the installation. It is not necessary to replace any cables already in situ.
Claims of compliance must be as described in Clause 3.2 of PD 6662: 2010 with the exception of:
a. Products for which PD CLC/TS 50131-2-8:2012 is applicable must be marked in accordance with BS EN 50131-1.
b. For BS 4737-3.30: 2015 no extra marking requirements apply other than those specified within that standard.

Cabling not conforming to BS 4737-3.30: 2015 may be used for contracts entered into up until 31st March 2016.

***The following warning must be in the system design proposal and as-fitted document:***

***"IMPORTANT If using a remote device to remotely set/unset your intruder alarm system, your attention is drawn to the fact that whenever a premises is unattended but its intruder alarm system(s) is (are) not fully set, any related insurance cover might be inoperative. For advice on this matter, it is recommended that you consult your insurer(s)."***

# Brand Evolution


Celebrating twenty years of Innovation

## Glossary of Terms used in this Booklet

| | | |
|---|---|---|
| **ARC** | - | Alarm Receiving Centre |
| **ATS** | - | Alarm Transmission System |
| **BS** | - | British Standard |
| **CIE** | - | Control and Indicating Equipment (control panel/keypad) |
| **DURESS** | - | An alternate code that when used triggers a silent PA |
| **EN** | - | European Norm or Standard |
| **HUA** | - | Hold Up Alarm (Personal Attack or PA) |
| **I&HAS** | - | Intruder and Hold Up Alarm System |
| **IAS** | - | Intruder Alarm System |
| **IP** | - | Internet Protocol |
| **LED** | - | Light Emitting Diode |
| **NGN** | - | Next Generation Network |
| **NPCC** | - | National Police Chiefs' Council |
| **PD** | - | Published Document (not always a standard) |

## WHAT'S THE STORY?

PD 6662:2010 is the UK scheme for the application of European standards for intrusion and hold-up alarm systems.

## TAMPER TAMPER!

All conditions that allow an option of fault or "tamper" (see BS EN 50131-1:2006+A1, Table 20) must be processed as tamper conditions
(PD 6662:2010 A.4)

Tamper detection of removal from mounting required for all wired I&HAS components in Grades 3 and 4, this is optional for junction boxes and magnetic contacts at Grade 3
(EN50131-1 8.7.2 Table 12 and 13)

If a Tamper causes an unconfirmed alarm, a Tamper event only to be notified at the ARC
(BS8243 2010 H.7.1)

A Tamper and an intruder received by the ARC will be treated as a confirmed alarm
(BS8243 2010 H.7.1)

All components used throughout the installation are to comply with the grade of the system and be marked by the manufacturer.
(PD 6662:2010)

## IT'S ALL ABOUT THE PD 6662/EN 50131 GRADE

Connection to the mains supply should be via an un-switched fused spur in Grade 2. Occasionally a connection via an un-switched mains socket can be made provided the inadvertent removal of the plug is prevented and the customer agrees to the use of the socket
(DD CLC/TS50131-7 H.21 Informative)

Battery capacity can be worked-out by multiplying both the stand-by and alarm current draw by the stand-by and alarm times respectively. This should be done at the design stage. Consider allowing a 20% deficit in battery life
(PD6662 Annex B.4)

Written agreement to confirm customers' acceptance where level 3 (engineer) access is necessary, level 2 permission not required every time
(PD6662 A.3 Normative)

Grade 1T is a grade for systems with internal sounders but no external siren. Signalling path to be tested at least every 32 days
(PD6662 Annex B.2 Informative)

***Check that Grade 3 detection devices come with mount tampers. Panel manufacturers should have implemented software changes – check it out!***

**BS8243:2010 SUPERSEDES DD243:2004**

**WHAT DOES THIS MEAN WHEN INSTALLING SYSTEMS?**

**SETTING/UNSETTING OF SYSTEMS**

In systems that use a digital key (fob) for unsetting, only one detector 'off' the entry route is required for a confirmed signal to be produced following entry to the premises. The confirmed alarm would be transmitted at the expiry of both the entry time (maximum 45s) and the alarm notification time (minimum 30s)
(BS8243 2010 6.4.5)

An audible indication should be heard throughout the exit/entry route and outside the premises to confirm that the system is set
(TS 50131-7 7.3.4)

Grade 3 or 4 should not include an indication of set/unset status – it is acceptable for Grades 1 & 2
(8.5.2 of BS EN 50131-1:2006+A1:2009)

Where it is not practicable to initiate the entry time with a door contact e.g a glass door, an alternative means of detection can be used e.g. a curtain PIR, provided the area of coverage will not be blocked by stock or other objects
(BS8243 6.4.4 and 6.4.5)

Maximum unset time is 45 seconds
(EN50131-1 8.3.8.2)

Deviation during the entry period is immediately notified by a Warning Device or indicated on-site
(BS8243 2010 6.4.5)

***Consideration should be given to the impact of telephone line providers, such as: NGNs, Broadband, Low Cost Routing and VOIP - it's all changing!***

**RISK ASSESSMENT & SYSTEM DESIGN PROPOSAL (SDP)**

Required prior to installation with any changes agreed in writing
(TS 50131-7  7)

Must include details of timing, set and unset method
(TS50131-7 Annex G)

Should include the ATS performance and Environmental Classification
(TS50131-7 Annex G)

Consider impacts of building location and contents.

**HOLD UP ALARMS (HUAs) OR PAs**

Response to new PAs need a separate URN
(NPCC Policy 2015)

Where the PA URN is deleted, a new URN will attract a new and separate payment (even if previously paid)
(NPCC Policy 2015 Appendix E)

If Police Response to PA is lost, it will need to be re-applied for with the addition of audible, visual, sequential or telephone confirmation
(NPCC Policy 2015 Appendix F)

Grade 2 portable PAs on Grade 3 installations does not result in overall downgrading of system to Grade 2
(PD6662 Annex B.1)

Whether PAs are portable or fixed they must be dedicated and consist of two separate trigger buttons
(BS8243 2010 4.5)

The use of Duress is limited to Grade 3&4 and must be signalled differently to PAs and not initiated with a key fob (ACPO policy). The limitation is that Grade 3 is by exception and would need to be applied for on a case by case basis with the local Police force
(NPCC Policy 2015 Appendix T.5)

*PA configuration example for confirming "hold-up" signals where limited format reporting must be "unambiguous". The use of "pin 7" in the example below is one method of achieving this:*
*PA (channel/pin 2) + Confirmed (pin 7) = Confirmed Hold-up*
*Intruder (pin 3) + Confirmed (pin 7) = Confirmed intrusion*
*PA (pin 2) + Intruder (pin 3) + Confirmed (pin 7) = Confirmed Hold-up*
*PA (pin 2) + Tamper (pin 6) + Confirmed (pin 7) = Confirmed Hold-up*
(BS 8243 2010 H.7.3 + H.3.2)

---

***Chat with your ARC to agree the above configurations - all installations are not the same!***

## MONITORING AND POLICE RESPONSE

ARC alarm filtering is set at 120 seconds (to allow for abort time)
(BS8243 2010 7.5.3)

To assist with false alarm management a maximum of 2 ‘policed’ remote resets are permitted in a rolling 12 month period and confirmed alarms can be restored by the alarm company only - not the end user
(BS8473)

Grade 3&4 tamper alarms can only be restored by access level 3 users
(EN50131-1 8.3.9 Table 6)

Grade1 and Grade 2X must not be used for Police Response systems
(PD6662 Annex A.2 Normative)

Timed exit must not be used for confirmed alarm systems that require a Police Response
(BS8243 2010 6.3)

Recommendation that it is preferable for the CIE, signalling and network equipment to be located in an area where a confirmed activation will be generated
(BS8243 2010 5.1.3)

The ARC address does not need to be documented
(PD6662 Annex B.5)

In instances where a multi-action PA is used and two separate PA signals are received by the ARC, within the confirmation time (between 8 hours – 20 hours), it would be designated as a confirmed PA alarm
(BS8243 2010 5.4.1.2)

***Fault reporting times EN50136-1:2012:***

***Dual Path***
***Grade 2: 50hrs***
***Grade3: 60mins***
***Grade 4: 6mins***

***Single Path***
***Grade 2: 25hrs***
***Grade 3: 30mins***
***Grade 4: 3mins***

## COMMISSIONING AND MAINTENANCE

The audible indication for walk test must be distinguishable from an alarm generated by a warning device
(EN50131-7)

Checklist for onsite commissioning (in addition to existing recommendations): record the resistance of the detection equipment and continuity of bus-wired devices, site configuration data, detector location, operation and coverage, tamper detection, environmental conditions, soak test, clock, event log and correct operation of all communications paths to ARC
(DD263 Annex A)

Remote check (off site) must be done on a secure computer within the alarm company premises or the ARC and include an authorisation and authentication process e.g. a VPN (secure data connection). Records must be kept for 15 months
(DD263 Section 4)

A full handover to the end user that includes a demo and explanation of ARC/Police response must take place and left in a document upon completion
(DD263 Annex A)

Emergency repair service must be offered 24/7 with attendance to site within 4 hours. This can be extended for Bells-only systems or by written agreement with the customer
(DD263 7 Corrective maintenance)

***Options available for on-site or remote maintenance must not create false alarms. Customer and ARC must be warned about any effects that testing may have on the system***
**(DD263 6.3.1 General)**

# CSL

CONNECTED

SECURE

LIVE