National Security Inspectorate
Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY
E: nsi@nsi.org.uk | W: nsi.org.uk

Dated: 12 October 2017

To:
1. All NSI NACOSS Gold and System Silver Companies
2. Applicant Companies who wish to gain approval for the above schemes of approval

TECHNICAL BULLETIN No: 0040

Guidance on the implementation of PD 6662:2017, the British Standards Institution Published Document Scheme for the application of European Standards for intrusion and hold-up alarm systems, including guidance on the implementation of BS EN 50131-1:2006+A2:2017 and BS 9263:2016

(Supersedes PD 6662:2010)

PD 6662:2017 shows a publication date of the 31st August 2017 and is available through licensed outlets including NSI who can supply copies at a discounted rate. The new standard supersedes PD 6662:2010, which will be withdrawn on 31 May 2019.

PD 6662 contains requirements and guidance on the implementation of the design, installation, commissioning and maintenance of Hold-Up Alarm Systems (HAS), Intruder Alarm Systems (IAS) and Intruder and Hold-Up Alarm Systems (I&HAS) in the United Kingdom. The document references a number of British and European Standards which provide detailed system requirements and associated component standards. Organisations that demonstrate compliance with PD 6662:2017, and also satisfy the relevant NSI criteria for approval, will be approved for the following scope:

"The Design, Installation and Maintenance of Electronic Security Systems including Access Control, CCTV Systems and Intruder Alarms".

Implementation timescale

The Published Document will be subject to a transition period and the installation and maintenance practices of existing and applicant approved companies will have to comply with the requirements of PD 6662:2017 for all new contracts entered into from 1 June 2019.

Status of PD 6662 and associated BS Codes of Practice

Although issued as a British Standards Institution Published Document, compliance with the recommendations given in PD 6662:2017 are mandatory for companies wishing to maintain NSI approval with respect to the design, installation and maintenance of intruder and hold-up alarm systems (I&HAS), intruder alarm systems (IAS) and hold-up alarm systems (HAS), subject to any additional clarifications and guidance included within this Technical Bulletin or issued subsequently.

The recommendations given in PD 6662:2017 must therefore be regarded as requirements in relation to NSI approval for the design, installation of I&HAS, IAS and HAS. This principle applies to all other Codes of Practice called-up by PD 6662:2017.

Details of the changes

General

The intention of this Technical Bulletin is to highlight the changes in PD 6662:2017 and the associated reference documents and explain how these will affect installation and maintenance practices. Some relevant NSI Circular Letters are cross referenced in this document.

The primary reason for the publication of the latest revision of PD 6662 is the publication an amendment BS EN 50131-1:2006+A2:2017 Alarm systems, Intrusion and hold-up systems, System requirements.

Additionally PD 6662:2017 now references British and European standards that have been subject to amendment or have been published since the publication of PD 6662:2010.

The requirements of IA 1501:2015 Industry Agreement on the Interim Update of PD 6662:2010 (NSI Circular Letter NSI 012/15 dated 21 July 2015) have also been included in PD 6662:2017.

A number of standards referenced within PD 6662:2017 are now not dated, i.e., the publication date of the standard has been omitted. This means that, should one of these documents be amended, there will be no requirement to update PD 6662:2017 and the requirements of the later document will apply immediately, subject to any transitional arrangements. As these documents are amended, NSI will publish either a Technical Bulletin or Circular Letter to explain the changes, the transition arrangements and the effect these may have on an approved company's installation and maintenance practices.

Highlighted under the clauses of the new Standards

Comments under each clause detail the relevant standard and/or changes when compared with the corresponding clause in the previous standard.

Where the actual wording of the standard is quoted, it is reproduced in bold text.

Where it is considered relevant to further clarify the specified requirement, additional guidance is included in italics.

We will consider alternative methods of achieving compliance with specified requirements where these can be demonstrated to be equivalent.

PD 6662:2017

Clause 1 Scope

There are no significant changes to the Scope.

Clause 2 Terms, definitions and abbreviations

The definition of "remote device" taken from IA 1501:2015 has been added:

2.1.1 remote device

type of remote non-I&HAS interface including the capability for the user to set and unset an IAS

Clause 3 Scheme content

3.1 System standards

Noting that a number of the system standards are now undated, the default transition time has been set at 12 months from the date of publication by BSI of a more recent standard.

The requirements of dated system standards will continue to apply until PD 6662:2017 is revised or publication of an interim agreement document incorporates any new or amended requirements into the PD 6662 scheme.

The following system standards are now called up in PD 6662:2017:

BS 8243, *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice*

This document is now undated.

BS 8473, *Intruder and hold-up alarm systems – Management of false alarms – Code of practice*

This document is now undated.

BS 9263, *Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice*

This document is undated and is a revision of ***DD 263 Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice.***

BS EN 50131-1:2006+A2:2017, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

This document has been revised and replaces **BS EN 50131-1:2006+A1:2009, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements.***

DD CLC/TS 50131-7:2010, *Alarm systems – Intrusion and hold-up systems – Part 7: Application guidelines*

This document has been revised and replaces ***DD CLC/TS 50131-7:2008 Alarm systems – Intrusion and hold-up systems – Part 7: Application guidelines.***

PD 6662:2017 (Annex A), *Scheme for the application of European standards for intrusion and hold-up alarm systems*

This document has been revised and replaces ***PD 6662:2010 (Annex A), Scheme for the application of European standards for intrusion and hold-up alarm systems.***

The following standards for alarm transmission systems have not been included:

BS EN 50136-1-1:1998+A2:2008, *Alarm systems – Alarm transmission systems and equipment – Part 1-1: General requirements for alarm transmission systems*

BS EN 50136-1-2:1998, *Alarm systems – Alarm transmission systems and equipment – Part 1-2: Requirements for systems using dedicated alarm paths*

BS EN 50136-1-3:1998, *Alarm systems – Alarm transmission systems and equipment – Part 1-3: Requirements for systems with digital communicators using the public switched telephone network*

BS EN 50136-1-4:1998, *Alarm systems – Alarm transmission systems and equipment – Part 1-4: Requirements for systems with voice communicators using the public switched telephone network*

BS EN 50136-1-5:2008, *Alarm systems – Alarm transmission systems and equipment – Part 1.5: Requirements for Packet Switched Network PSN*

The requirements of these standards have been replaced by BS EN 50136-1:2012 Alarm systems – Alarm transmission systems and equipment Part 1 General Requirements for Alarm transmission systems, which is called up in BS EN 50131-1:2006+A2:2017.

Clause 3.2 Component standards

Noting that most **BS EN 50131-X** component standards and **BS 4737-3.30** are now undated, the default transition time has been set at 2 years from the date of publication by BSI of a more recent standard.

*The requirements of the remaining **BS 4737-3.X** component standards, which are dated, will continue to apply until PD 6662:2017 is revised or publication of an interim agreement document incorporates any new or amended requirements into the PD 6662 scheme.*

The following new component standards are called up in PD 6662:2017:

BS 4737-3.30, *Intruder alarm systems in buildings – Part 3: Specifications for components – Section 3.30: Specification for PVC insulated cables for interconnecting wiring*

BS EN 50131-2-7-1, *Alarm systems – Intrusion and hold-up systems – Part 2-7-1: Intrusion detectors – Glass break detectors (acoustic)*

This replaces DD CLC/TS 50131-2-7-1:2009, Alarm systems – Intrusion and hold-up systems – Part 2-7-1: Intrusion detectors – Glass break detectors (acoustic).

BS EN 50131-2-7-2, *Alarm systems – Intrusion and hold-up systems – Part 2-7-2: Intrusion detectors – Glass break detectors (passive)*

This replaces DD CLC/TS 50131-2-7-2:2009, Alarm systems – Intrusion and hold-up systems – Part 2-7-2: Intrusion detectors – Glass break detectors (passive).

BS EN 50131-2-7-3, *Alarm systems – Intrusion and hold-up systems – Part 2-7-3: Intrusion detectors – Glass break detectors (active)*

This replaces DD CLC/TS 50131-2-7-3:2009, Alarm systems – Intrusion and hold-up systems – Part 2-7-3: Intrusion detectors – Glass break detectors (active).

BS EN 50136-2, *Alarm systems – Alarm transmission systems and equipment – Part 2: Requirements for Supervised Premises Transceiver (SPT)*

This replaces the BS EN 50136-2-X:1998 series of standards.

BS EN 50131-2-8, *Alarm systems – Intrusion and hold-up systems – Part 2-8: Intrusion detectors – Shock detectors*

This replaces BS 4737-3.10:1978, Intruder alarm systems in buildings – Part 3: Specifications for components – Section 3.10: Vibration detectors.

Clause 3.3 Alternative component standards

Additionally components certified to the following technical specification standards may be specified within a PD 6662:2017 installation.

PD CLC/TS 50131-2-9, *Alarm systems – Intrusion and hold-up systems – Part 2-9: Intrusion detectors – Active infrared beam detectors*

PD CLC/TS 50131-2-11, *Alarm systems – Intrusion and hold-up systems – Part 2-11: Intrusion detectors – ALDDR (Active Laser Detector Responsive to Diffuse Reflection)*

Clause 3.4 Interconnecting wiring

As detailed in IA 1501:2015, where a security company or their subcontractors are responsible for the installation of new interconnecting wiring, this must comply with the requirements of BS 4737-3.30 (see Clause 3.2).

There is no requirement to replace any nonconforming cable that is already in situ. However, where nonconforming cable is utilised this should be noted in the system design proposal or as-fitted documentation.

Clause 4.1 Claims of compliance

Clause 4.1 Systems

This includes the need for any claim that the scheme described in PD 6662:2017 has been followed, to state that **the I&HAS conforms to PD 6662:2017 at the security grade and notification option applicable to the system**.

Clause 4.2 Components

The first paragraph has been modified to include any PD CLC/TS referenced in 3.2 or 3.3.

The wording of the second paragraph has changed to:

If a BS referenced in 3.2 is applicable to the component, the component should conform to that standard and be further assessed to the applicable requirements of BS EN 50131-1 and BS EN 50130-5. The manufacturer should then issue a statement that the product "is suitable for use in systems installed to conform to PD 6662:2017 at Grade N and environmental class Y".

Examples of BS references include the BS 4737 series. The main clarification is the assessment by the manufacturer to the applicable requirements of BS EN 50131-1 and BS EN 50130-5 Alarm systems – Part 5: Environmental test methods.

The wording of the third paragraph has changed to:

If no standard within 3.2 is applicable to the component, the component should be assessed to the applicable requirements of BS EN 50131-1 and BS EN 50130-5. The manufacturer should then issue a statement that the product "is suitable for use in systems installed to conform to PD 6662:2017 at Grade N and environmental class Y".

Again, the main clarification is the assessment by the manufacturer to the applicable requirements of BS EN 50131-1 and BS EN 50130-5.

Clause 5 Identity cards

The requirement has changed so that only those company personnel **'who might be required to prove their credentials when carrying out their duties, should be issued with an identity card'.**

This removes the requirement for office based staff, who do not have a need to prove their credentials, to be issued with identity cards.

PD 6662:2017 Annex A

A.2 Police response

The requirement remains the same. However, BS EN 50131-1:2006+A2:2017 Table 10 now includes an option for a 'bells only' Grade 2 system, designated as '2E'. This replaces any previous reference to '2X' systems in PD 6662:2010.

Systems installed to Grade 1 (all Options) and Grade 2E under PD 6662:2017 must not be used to initiate police response.

A.5 Requirements (applicable to systems installed in compliance with BS 8243) for setting and/or unsetting using a remote device as a "Remote Non-I&HAS Interface"

These requirements for the use of remote devices, such as mobile phones, were previously published in Industry Agreement IA 1501:2015 and are now incorporated in PD 6662:2017. NSI Circular Letter NSI 012/15 has further details about IA 1501.

PD 6662:2017 Annex B (informative) UK specific guidance

The following clauses from PD 6662:2010, Annex B, have not been included in PD 6662:2017 Annex B:

Grade 1, Option T I&HAS

Systems installed to this standard will continue to be compliant to PD 6662:2010 and earlier. However, Grade 1 Option T systems are not available under PD 6662:2017.

Grade 1 Option C in Table 10 of BS EN 50131-1:2006+A2:2017 is similar to Grade 1 Option T in the sense there is a single path ATS and no mandatory audible warning devices.

Grade 2, Option X I&HAS

The requirements of this standard, which is the option for "warning devices only" in Grade 2, are now included at Option 2E in BS EN 50131-1:2006+A2:2017 Table 10.

When issuing NSI Certificates of Compliance for these systems, you should select the following parameters from the options in Part 4 of the Schedule:

4.1	Type of System & Standard/Code of Practice applicable	**EA**
4.2	Security Grade of System	**2**
4.3	Grade of Notification	**2**
4.4	Description of Notification	**EA**
4.5	Type of Premises	**B or C or E** (as applicable)

BS EN 50131-1:2006+A1:2009, 8.3.5, Prevention of setting

This clause is no longer needed due to lack of conflict.

DD CLC/TS 50131-7:2008, Annex B.6, System design

The requirement in DD CLC/TS 50131-7:2008, B.6 **"psychological problems of persons after robbery"** was deleted from DD CLC/TS 50131-7:2010.

Therefore this clause is no longer needed.

PD 6662:2017 Annex C (informative) Additional guidance

The following clause from PD 6662:2010, Annex C, has not been included in PD 6662:2017:

BS EN 50131-1:2006+A1:2009, 8.6, Notification

BS EN 50131-1:2006+A2:2017 Table 10 has been modified to reflect the terminology and categorisation of Alarm Transmission Systems (ATS) in BS EN 50136-1, which defines an ATS as either Single Path (SP) or Dual Path (DP). Table 10 clarifies the ATS requirements for the system grades and options in BS EN 50131-1. Further explanations of the changes to BS EN 50131-1:2006+A2:2017 Table 10 are included later in this document.

Therefore this clause is no longer needed.

BS EN 50131-1:2006+A2:2017

General

Although largely editorial, there are a number of changes to BS EN 50131-1 which will require you to consider the configuration options available to you when designing and installing a system.

These changes are:

1. The introduction of the requirements of BS EN 50136-1 in terms of amending the description of ATS types of notification in Table 10 and the introduction of three further notification options. See Table 10 BS EN 50131-1:2006+A2:2017.
2. The introduction of Alarm Transmission Path (ATP) faults, which are distinct from Alarm Transmission System (ATS) faults and the means to set up options for the notification, indication, management and recording of these faults.
3. Addition of a requirement to prevent test indications being observed at access level 1 in Grade 3 and 4 systems.
4. Modification of requirements on detection of masking.
5. Clarification of requirement to display all mandatory indications at one CIE/ACE.
6. Addition of requirements to enable users to be able to determine the identity of detectors that have caused an alarm condition.
7. Modification of the notes in Table 12 Tamper detection – Means to be detected, replacing the types of detectors which Table 12 applies to.

Editorial

Table 11 has been deleted as it is no longer required. Therefore every subsequent Table number has decreased by 1. However, there are errors within the standard as this change has not been noted in some of the text within the document, e.g., references to Table 22 have not be amended to Table 21 and care should be taken when cross referencing between text and tables.

Clause 2 Normative references

BS EN 50136-1-1 has been deleted and replaced with BS EN 50136-1.

All other references have been relegated to 'NOTE' status within the document and have been deleted from the references and are now included in a new Bibliography.

Amendments to Clause 8.6 and Table 10

Clause 8.6 Notification has been rationalised and sub-clauses **8.6.1 General, 8.6.2 ATS Notification, 8.6.3 Warning Device Notification and 8.6.4 Notification – Other** have been introduced to compartmentalise the various means of notification. No requirements have been amended in Clause 8.6.

The reference to EN 50136-1-1 has been replaced with EN 50136-1. This has modified the ATS notification requirements within Table 10, which is reproduced in Appendix 1. Table 10 now includes Option 2E which replaces Option 2X and two additional dual path options at grades 2 (2F) and 3 (3E) which have faster reporting times. These new notification options are highlighted in Appendix 1.

The addition of the 2E option has removed the requirement for the 2X option in PD 6662. This will not affect the issue of NSI Certificates of Compliance for 'bells only' systems and they will continue to be will certificated as previously (see details in PD 6662:2017 above).

The referencing of EN 50136-1 has clarified the requirements for ATS on I&HAS. Previously there were two interpretations of the ATS requirements in Table 10, Option C, which were (a) both ATS described in Table 10 were wholly independent of each other or (b) that each ATS was part of a combined Dual Path (DP) solution; both interpretations were accepted as valid, which caused confusion when determining the requirements to notify users of ATS faults.

The modified Table 10 makes it clear that the (b) interpretation, i.e., an ATS may consist of either one or two Alarm Transmission Paths (ATP), is intended to be applied.

The amendment of Table 10 does not affect the completion of NSI Certificates of Compliance as the option for the selection of one ATS with two transmission paths (ATP) is still available. However, with the addition of the 2F option, which introduces a DP2 option at Grade 2 (previously only an option at Grade 3C) systems that may have been certificated as Grade 2 with Grade 3 notification should now be certified as Grade 2 with Grade 2 notification, if a DP2 option ATS is installed. Details of the notification options available for each system grade should be available from the ATS provider.

Table 11, which relates to the various parameters associated with the ATS in the previous version of BS EN 50131-1, has been deleted and you should refer to BS EN 50136-1 for specific details on ATS performance.

Amendments to include Alarm Transmission Path Faults

3.1.77

alarm transmission path

route an ATS alarm message travels between an individual I&HAS and the annunciation equipment at its associated ARC

Note 1 to entry: The ATP starts at the interface between the AS and SPT and ends at the interface between the RCT and AE. For notification and surveillance purposes the reverse direction may be used.

3.1.85

alarm transmission system fault

fault that occurs when all ATPs are not available

Faults on ATS are now classified as ATP faults and ATS faults. An ATP fault on a Single Path (SP) ATS or complete failure of both ATP of a Dual Path (DP) ATS are ***alarm transmission system faults.*** *These have to be indicated, notified, managed and recorded as previously required by BS EN 50131-1.*

The introduction of the term ***alarm transmission path*** *allows the requirements for the indication, notification, management and recording of events relating to single ATP failures on a DP ATS to be clearly defined in BS EN 50131-1. The amendments relating to these requirements are listed below.*

There may be benefit in having an agreement with the customer about the configuration of the I&HAS in relation to ATP faults as insurers may be interested in this policy and this could be something to add to the System Design Proposal.

Clause 8.1.4 Recognition of faults

Table 1 Faults has been amended to include a new fault condition, 'Alarm transmission path' together with an amendment to note [a], see below.

Table 1 – Faults				
Faults	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**
Alarm transmission path[a]	**Op**	**Op**	**Op**	**Op**
[a] *EN 50136-1:2012, Table 5 optionally allows for reporting of ATP failure to the CIE. If the SPT and the CIE are configured to provide and process this fault or message then it shall be recognised.*				

The additional fault condition and amendment clarifies the circumstances in which a CIE has to indicate to the user when the SPT detects a single ATP fault in a dual path system. As this requirement is optional for all grades, the need to provide this notification and any subsequent management or recording is subject to the configuration of the system.

Clause 8.3.5 Prevention of setting

Table 4 has been amended to include the new fault condition in Table 1, 'Alarm transmission path fault'.

Table 4 - Prevention of setting				
Prevention of setting	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**
Alarm transmission path fault	**Op**	**Op**	**Op**	**Op**

The CIE must be configured to prevent setting if processing of this fault is enabled, see Table 1.

Clause 8.3.6 Overriding prevention of setting

Table 5 has been amended to include the new fault condition in Table 1, Alarm transmission path fault'.

Table 5 - Overriding of prevention of setting conditions				
Overriding of prevention of setting conditions	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**
Alarm transmission path fault	**Access level 2**	**Access level 2**	**Access level 2**	**Access level 2**

The CIE must be configured to permit users with access level 2 to override a single path fault at all grades in a dual path system if processing of this fault is enabled, see Table 1.

Clause 8.5.1 Indications - General

Amendment to paragraph 5

Deleted

'Where an I&HAS is required by its grade and notification option to have more than one alarm transmission system, a detectable fault on any of the transmission systems should be indicated to the person setting the system.'

Inserted

'Where the SPT and CIE have been configured to recognise ATP faults (see Table 1), such faults shall be indicated to the user at the time of setting'.

This provides clarification of indication required to be presented to the user when setting the system where single ATP faults on dual path ATS may exist.

Clause 8.10 Event recording

Table 21 now contains a new requirement for ATP faults to be recorded on the system.

Table 21 - Event recording - Events to be recorded				
Events	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**
ATP fault	**Op**	**M**	**M**	**M**

As the reporting of ATP faults to the CIE is optional at all grades in Table 1 (see above), these ATP faults need only be recorded in Grades 2, 3 and 4 if the option to report ATP faults is chosen.

Clause 8.3.12 Test

At grades 3 & 4 indications for test purposes (e.g. on detectors) are not permitted at access level 1.

The earlier standard only had requirements for test indications on detectors to be capable of being turned on and off locally (Grades 1 & 2) or remotely (Grades 3 & 4).

These requirements remain and, to conform to PD 6662:2017, Grade 3 and 4 I&HAS will now have to be configured so that all test indicators are not able to be viewed by users at access level 1.

You may have to refer to manufacturer's documentation to identify which indications on components are considered to be test indications.

Amendment to Masking requirements of detectors

Clause 8.2.1 Masking

Previously the clause referred to movement detectors. However, as other detectors may be subject to masking the clause was amended to include this possibility.

In grades 3 & 4 I&HAS if the detector mechanism employed in a detector includes technology that would allow the detector to be masked, means shall be provided to detect masking, or the detector shall be immune from masking

NOTE Examples of such detectors include movement detectors, shock detectors and glass break detectors

This previously applied only to movement detectors but has been modified to include any detector that may be masked/desensitised in some way to prevent them from operating correctly. This is primarily an issue for manufacturers but you should be aware of these requirements when looking for Grade 3 and 4 products.

Amendment to Processing of ATS Fault Notifications

Clause 8.4 Processing

New note in Table 7

NOTE 6 For the purpose of avoiding duplicate fault notifications, where the ATS includes the monitoring of the ATP or ATS by the ARC then remote notification of an ATS or ATP fault by the CIE is not required.

This NOTE assumes the SPT will manage failures in the ATS and notify the ATSP (Alarm Transmission Service Provider) and ARC as required. This function may need to be configured in the CIE during system set up. Systems reporting twice will not have failed to meet any requirement but this may lead to inaccurate processing of this information at the ARC and could cause false alarms.

Amendments to 8.5.1 General (Indications) - Duplicate indications

Clause 8.5.1 General

Amendment to paragraph 4

'Further' deleted **'Duplicate'** inserted. Now reads; **'All mandatory indications required by this clause shall be located in at least one CIE or ACE. Duplicate indications may be provided at other locations'**

*Clarification of an ambiguity in the original requirement to ensure **all** mandatory indications are displayed by at least one CIE or ACE on the system and are only to be distributed to other CIE or ACE in the system as duplicates of these indications, i.e., additional CIE or ACE in the system cannot display mandatory notifications which are not also displayed at the main/primary CIE or ACE.*

Amendments to Clause 8.5 Indications, 8.5.1 General, 8.5.2 Availability of indications, 8.5.4 Identification of cause of intrusion alarm condition & Tables 8 and 9 – Duplicate indications and Intrusion detection indication

Clause 8.5.1 General

Amendments to Table 8

Table 8 – Indication				
Indications	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**
Delete				
Individual intrusion detector indication (see 8.5.4) [a]	**Op**	**Op**	**M**	**M**
Insert				
Intrusion detector identification (see 8.5.4 and NOTE 2)	**M**	**M**	**M**	**M**

Inserted as a Note in Table 8

NOTE 2 The intrusion detector identification is intended to enable the user to determine the cause of the intruder alarm condition

Footnotes [a] and [d] in Table 8 have been deleted. Footnote [a] related to detectors with processing capabilities and is now included in the requirements in clause 8.5.4. Footnote [d] was no longer considered to be necessary. The remaining footnotes have been renamed to address this.

Clause 8.5.2 Availability of indications

Table 9 - Indications available during the set and unset status at access level 1								
Indications	**G 1**	**G 1**	**G 2**	**G 2**	**G 3**	**G 3**	**G 4**	**G 4**
	Set	**Unset**	**Set**	**Unset**	**Set**	**Unset**	**Set**	**Unset**
Insert								
Intrusion detector identification (see 8.5.4)	**Op**	**Op**	**Op**	**Op**	**Op**	**Op**	**Op**	**Op**

Amended

Clause 8.5.4 Identification of cause of intruder alarm condition previously **Indication – intrusion detectors**

Clause 8.5.4.1 General for IAS

I&HAS shall provide means to determine which detector caused an intrusion

Clause 8.5.4.2 Intrusion detectors including processing capability

For intrusion detectors which include processing capability the user shall be capable of determining the identity of the individual detector responsible for causing the alarm conditions (see Table 8).

Clause 8.5.4.3 Intrusion detectors not including processing capability

Intrusion detectors without processing capabilities are permitted to share a common means of indication. Not more than 10 such detectors are permitted to share a common means of indication.

The amendment in **Table 8** and general statement in the amended clause **8.5.4.1 General for IAS** introduces a new requirement that at all grades detectors with a processing capability have to indicate to a user at the CIE and ACE that they have been activated. Previously this was only required at grades 3 & 4.

The amendment in Table 9 includes a new requirement to optionally indicate this information to a user at level 1 access in all grades in both set and unset state.

The requirements in the new clauses 8.5.4.2 and 8.5.4.3 are clarifications/reiterations of statements in the previous version of 8.5.4 and do not modify the original requirements.

I&HAS at all grades must now be configured to indicate the individual or group of detectors (dependent on processing capability) that have caused an intrusion alarm at the CIE and ACE. The availability of this indication is optional at access level 1 and mandatory at access levels 2 and above.

Amendment to Table 12 Tamper detection – Means to be detected

Footnotes amended

Table 12 Tamper detection – Means to be detected

Footnote a **'When located outside the supervised premises'** previously applied to '**Penetration of audible WD'** and '**Penetration of ACE/CIE/SPT'** in Grade 4 systems. This now applies optionally at Grades 1, 2 & 3 to the '**Penetration of audible WD'** and optionally at Grades 1, 2 & 3 for the '**Penetration of ACE'**.

Footnote c relates to a list of components which are optionally required to detect **'Removal from mounting - Wired system components'.** This list has been has been expanded to include all the following; **junction boxes, opening contacts (magnetic), lock state contacts, bolt contacts, hold-up devices, concealed flush mounted shock detectors, break glass detectors designed to be secured to glass.**

It is mandatory for wired system components to include means to detect removal from mounting except in the case of the listed components where the requirement is optional.

Footnote d **'This requirement does not apply to ACE of Type A'** refers to **'Opening by normal means' at all grades.**

It is not necessary for ACE of Type A to include means to detect opening by normal means.

Definition of Type A components:

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 (EXAMPLE: potted device);

The amendments to Table 12 clarify but do not fundamentally change any requirements within the standard.

BS 9263:2016

BS 9263 - Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice replaces **DD 263 Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice**.

DD (Draft for Development) 263 was converted to BS 9263 in 2016 and has undergone minor revisions. Details of the changes are detail below.

Clause 4.2 Initialization of connection

Amended

c) Manual or automatic, remote: Remote service personnel manually initiate a connection from a secure computer to the I&HAS or the secure computer initiates the connection automatically for the purposes of remote support or remote system checks.

Amendment permits a secure computer to carry out remote support or system checks as part of a scheduled maintenance plan or in response to a notified fault without the intervention of any service personnel.

Deleted

c) 1) of DD 263:2010 The I&HAS identifies the secure computer used, (example by IP address) or its location (example by identification of fixed telephone line).

Security measures suggested are not considered to be secure enough as it is possible to defeat both these means of identifying the secure computer by spoofing either the IP address or the telephone number. Therefore this means of authentication of the secure computer, which includes dial back, is no longer permitted.

Clause 6.3.2 Application of Annex B.3

Amended

'When applying remote system checks in accordance with Annex B, B.3, the following checks should be carried out',

The wording of the opening paragraph in clause 6.3.2 has been amended to make remote system checks detailed in Clause 6.3.2 a stated requirement, not a consideration. Therefore security companies using remote system checks as part of their preventive maintenance regime must ensure that all requirements stated in clause 6.3.2 are carried out.

Clause 9 Documentation, audit trail and records

New

h) monthly and annualized performance records of all preventative maintenance.

This is a new requirement and, whilst not prescriptive in what is required in terms of data collected, you should retain documentation with sufficient detail in the performance records to determine whether the requirements of ***Clause 6.4 Frequency*** *(of preventative maintenance) and* ***Table 1 Minimum frequency of preventive maintenance*** *have been met.*

Annex A - Commissioning of an I&HAS

New

The following components have been added to Row 3 of **Table A 1: power supply units, expanders, remote key pads and junction boxes**

Introduces a new requirement to label interconnections at the following components: CIE, power supply units, expanders, remote key pads and junction boxes. Previously this requirement only applied to the CIE.

Amended

Check that there is adequate standby battery capacity to meet the requirements of the applicable standard the system was installed to

Amendment to clarify the commissioning requirements for system standby batteries.

Annex B - Preventative maintenance checks

Amended

B.1 General

Preventative maintenance should be in accordance with B.2 (Site visit) or B.3 (Remote system checks) and documented in accordance with Clause 9.

Introduces a requirement for security companies to document preventive maintenance in accordance with the requirements of Clause 9.

Amended

B.2 Site visit

a) ensure that the installed system meets the as-fitted document;

Clause amended to make the requirements of this task explicit.

New

b) tamper detection;

NOTE 1 Check at least one tamper for correct operation through to the CIE.

Note added to sub-clause b) to clarify requirements for testing of tamper detection during preventive maintenance.

New

c) setting and unsetting;

NOTE 2 Offer user(s) refresher system operation training, if required.

Note added to sub-clause c) to draw attention to need to offer refresher training. This may be a solution to a system where there are a significant number of false alerts generated during the setting and unsetting process.

New

e) power supplies, including any APS;

NOTE 3 See Annex C.

Note added to sub-clause e) to draw attention to Annex C Calculation of standby battery capacity

New

H) operation of WDs;

NOTE 4 Operation of self-powered WDs includes removal of hold-off voltage.

Note added to sub-clause h) to specify the requirement to test the removal of hold off voltages on WD.

B.3 - Remote system checks

Amended

c) check no adverse tamper or fault conditions exist on the system where the system has this capability;

Amendment made to clarify that some systems may not be able to meet this requirement.

Annex C Calculation of standby battery capacity

New

This is a new informative Annex to provide guidance to installers and maintainers on how to calculate standby battery capacity. This does not introduce any new requirements.

Appendix 1

Table 10 - Notification requirements																		
Notification equipment	I&HAS Grade 1			Grade 2						Grade 3					Grade 4			
	Options			Options						Options					Options			
	A	B	C	A	B	C	D	E	F	A	B	C	D	E	A	B	C	D
Remotely powered audible WD	2	Op	Op	2	Op	Op	Op	Op	Op	2	Op	Op	Op	Op	2	Op	Op	Op
Self-powered audible WD	Op	1	Op	Op	1	Op	Op	1	Op	Op	1	Op	Op	Op	Op	1	Op	Op
ATS	Op	Op	SP1	SP2	SP2	DP1	SP3	Op	DP2	SP3	SP3	DP2	SP4	DP3	SP5	SP5	DP4	SP6

Key:
Op = Optional
SPn = Single Path Performance Category, DPn Dual Path Performance Category (Ref to EN 50136-1)
NOTE 1 Digits in cells specify the number of audible warning devices to be included by grade and option.
NOTE 2 The requirements included in each grade and option represent the minimum requirements. It is permissible to include additional WD or to select higher performance ATS in any grade or option, e.g. to achieve a shorter reporting time.