Security.Improved

Dated: **May 2011**
To: **All NACOSS Gold, Systems Silver and ARC Gold approved companies and applicants for NACOSS Gold, Systems Silver and ARC Gold approval**

TECHNICAL BULLETIN No. 0016

Guidance on the application of British Standards Institution Draft for Development DD 263:2010 – Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice

(Supersedes BSI DD 263:2007)

INTRODUCTION

This Technical Bulletin gives guidance on the application of British Standards Institution (BSI) Draft for Development DD 263:2010, which is about commissioning, maintenance and remote support of intruder and hold-up alarm systems (I&HAS).

DD 263:2010 ("the DD") is one of the standards called-up by PD 6662:2010.

The first (2007) edition of DD 263 was not adopted in the UK, partly due to its complexity. BSI then reviewed the 2007 edition and produced DD 263:2010.

The DD incorporates maintenance recommendations formerly included in BS 4737, *Intruder alarm systems in buildings*. The DD applies to all I&HASs installed to PD 6662:2010, PD 6662:2004, BS 4737, BS 6799 and BS 7042 from 1 June 2012 onwards.

This Technical Bulletin gives guidance on the application of DD 263:2010 ("the DD"), but does not attempt to compare DD 263:2010 with DD 263:2007.

The wording of the DD is paraphrased in a number of areas in this Technical Bulletin. Whilst every effort has been made to convey the true meaning of the DD, the actual wording of the DD prevails in situations where there might be a perceived conflict.

Please refer to DD 263:2010 for full details of the requirements.

SUMMARY OF KEY POINTS

1 DD 263:2010 ("the DD") came into effect on 31 May 2010 and is one of the standards called-up by PD 6662:2010.

2 There is a two-year timetable for the introduction of PD 6662:2010, which means that intruder and hold-up alarm systems (I&HASs) can be installed to PD 6662:2004 or PD 6662:2010 up until 31 May 2012. However, from 1 June 2012 all new I&HASs

must be installed to PD 6662:2010. See NSI Circular Letter Ref: 006/10 dated 1 June 2010 and NSI Technical Bulletin 0013 for more information about the introduction of PD 6662:2010.

3 The DD must be applied in full to all I&HASs meeting PD 6662:2010 irrespective of whether these PD 6662:2010 I&HASs are installed before or after 1 June 2012.

4 The DD can be applied to all I&HASs (PD 6662:2010, PD 6662:2004, BS 4737, BS 6799 and BS 7042) before 1 June 2012.

5 However the DD must be applied to all I&HASs (PD 6662:2010, PD 6662:2004, BS 4737, BS 6799 and BS 7042) from 1 June 2012 onwards.

6 Application of the DD results in harmonization of preventative and corrective maintenance from 1 June 2012 onwards as shown in Table 1 below:

Table 1 – Summary of standards for maintenance

INSTALLATION	**MAINTENANCE**	
Standard	**From 1 June 2010 to 31 May 2012**	**From 1 June 2012**
PD 6662:2010	DD 263:2010	DD 263:2010
PD 6662:2004	Annex D of PD 6662:2004 or DD 263:2010	DD 263:2010
BS 4737	Section 4.2 of BS 4737 or DD 263:2010	DD 263:2010
BS 6799	Section 4.2 of BS 4737 or DD 263:2010	DD 263:2010
BS 7042	Section 4.2 of BS 4737 or DD 263:2010	DD 263:2010

Note: You may need to review the wording of your maintenance contracts (if these contracts refer to BS 4737) before you move over to the DD.

7 The minimum frequency of preventative maintenance (site visits and remote system checks) is given in Table 6 on page 9 of this Technical Bulletin.

Note: PD 6662 Grade 1A, Grade 1B, Grade 1C, Grade 1T and Grade 2X systems are not suitable for police calling systems.

8 Commissioning applies to new I&HASs and does not apply retrospectively to I&HASs that are already operational. This is unless an I&HAS needs to be re-commissioned.

9 Remote system checks can be carried on all I&HASs (PD 6662:2010, PD 6662:2004, BS 4737, BS 6799, BS 7042), but only if these checks meet the DD. Therefore, it will not be possible to provide remote system checks to many older systems.

10 Remote support can be carried out on all I&HASs (PD 6662:2010, PD 6662:2004, BS 4737, BS 6799, BS 7042), but only if remote support meets the DD. Therefore it will not be possible to provide remote support to many older systems.

11 Conditions/restrictions relating to remote support functions are detailed in Table 7 on page 11 of this Technical Bulletin.

DETAILS ABOUT DD 263:2010

Details about DD 263:2010 ("the DD") are given below against the relevant clause of the DD. Guidance or comment about the DD is given in *italics*.

The Tables given in this Technical Bulletin may be copied, used and/or adapted for the purpose of meeting the DD.

1 SCOPE

The DD gives recommendations for the commissioning, on-site corrective and preventative maintenance, remote system checks and remote support of I&HAS.

The DD covers all intruder and hold-up alarm systems (I&HAS) under maintenance. This means I&HASs meeting PD 6662:2010, PD 6662:2004, BS 4737, BS 6799 and BS 7042.

2 NORMATIVE REFERENCES

Please refer to the DD for details of the normative references.

3 TERMS, DEFINITIONS AND ABBREVIATIONS

Please refer to the DD for details of the terms, definitions and abbreviations. For ease of reference a few of the terms and definitions are included below.

3.1.6 dialogue
electronic communication between the I&HAS and a secure computer resulting in an exchange of data

3.1.12 remote service personnel
personnel at a remote location operating the secure computer controlling a dialogue

NOTE This operation may be automated.

3.1.13 remote support
carrying out some or all the CIE functions of an I&HAS from a secure computer

3.1.14 remote system check
electronic check of the status of an I&HAS from a secure computer as part of preventative maintenance

3.1.15 secure computer
computer at a remote location used to access remote servicing or support functions, which are not accessible without applying security measures, so that unauthorized persons cannot gain access to data by normal means

*NOTE See **4.3** for authorization requirements.*

4 SECURITY OF COMMUNICATIONS FOR REMOTE SUPPORT AND REMOTE SYSTEM CHECKS

4.1 General

Remote support (see definition 3.1.13) and remote system checks (see definition 3.1.14) need to be carried out using a secure computer (see definition 3.1.15).

The interfaces to the secure computer need to meet the requirements of Annex C of BS EN 50131-3:2009.

Please obtain confirmation in writing from your suppliers that they comply with Clause 4 of the DD, including Annex C of BS EN 50131-3:2009, in terms of security of communications for remote support and remote system checks.

Explanatory notes about security of communications:

- *Access to the secure computer at the remote location needs to be restricted to authorized persons. The requirements for authorization are given in 4.3 of the DD.*
- *The permitted methods for initializing the connection between an I&HAS and a secure computer are given in 4.2 of the DD. However, initialization is not complete until communications have been authenticated (see next bullet point).*
- *Communications need to be authenticated before data is exchanged between the I&HAS and the secure computer. The requirements for authenticating communications are given in 4.4 of the DD.*
- *The requirements of information security are given in 4.5 of the DD.*

4.2 Initialization of connection

For ease of reference, the permitted methods of initializing the connection between an I&HAS and a secure computer are given in Table 2 below.

Table 2 – Methods for initialization of connection

METHOD	DETAILS
Automatic	The I&HAS initiates a dialogue (see definition 3.1.6) due to one of the following: • in response to a system event • at a pre-programmed time when remote system checks are scheduled
Manual, on site	A user or an alarm company service technician on site manually initiates a connection from the I&HAS to the secure computer.
Manual, remote	Remote service personnel (see definition 3.1.12) manually initiate a connection from a secure computer to the I&HAS. Use of this method at grade 3 of PD 6662 / EN 50131 is not permitted unless ONE of the following three safeguards is in operation: • the I&HAS identifies the secure computer (for example by the IP address) or the location of the secure computer (for example by identification of the correct telephone line) • information security measures are in place meeting sub-clause 4.5 of the DD • a user or an alarm company service technician on site confirms initialization of the connection Use of this method at grade 4 of PD 6662 / EN 50131 is not permitted unless information security measures are in place meeting sub-clause 4.5 of the DD.
Manual, remote with PSTN or ISDN ring-back	Remote service personnel (see definition 3.1.12) manually initiate a connection from the secure computer to the I&HAS. On receipt of the incoming call, the I&HAS drops the connection and initiates an automatic dial-back call to the secure computer.

4.3 Authorization

Please refer to 4.3 of the DD for full details about authorization.

Remote service personnel (accessing the communications software running on the secure computer) must be uniquely identifiable in the audit trail (for example by use of individual PIN codes). For security reasons, management procedures must be in place at the secure location to ensure that:

- if PIN codes are used for access to the communications software, the PIN codes are changed at regular intervals
- remote service personnel log out of the communications software before allowing other remote service personnel to use the software (so as to maintain the audit trail of who is using the software)
- remote service personnel log out of the communications software before leaving the secure computer unattended
- access to the secure computer and/or to the communications software is promptly barred to personnel leaving employment

4.4 Authentication of communication

Sub-clause 4.4 of the DD gives full details about authentication of communication.

4.5 Information security

Sub-clause 4.5 of the DD gives full details about information security.

5 INSPECTION, FUNCTIONAL TESTING AND COMMISSIONING

The I&HAS must be inspected and functionally tested to ensure that it operates correctly and meets the system design proposal (and the installation plan when such a plan is necessary) including any changes agreed with the client.

The I&HAS must be commissioned in accordance with clause 10 of DD CLC/TS 50131-7:2008 and with Annex A of the DD. The commissioning results must be recorded using a checklist similar to Table A.1 of the DD (see also Table 3 below).

Table 3 – Commissioning checks

Actions	Checked	Remarks
Check that the I&HAS has been installed and configured in accordance with the system design proposal (any deviations agreed in writing with the customer)		
Check the I&HAS complies with current industry standards and is to a high standard of workmanship		
Check that all interconnections are clearly labelled at the CIE		
Log resistance of detection interconnections or check continuity of bus wired interconnections		
Check every detector for correct operation through to the CIE		

Actions	Checked	Remarks
Check that all batteries in CIE/PS(s) are marked with the date of installation		
Log the current drawn by all power supplies with the I&HAS in quiescent and alarm states		
Remove the mains supply and check that the battery voltage of all equipment is within the specified limits and the I&HAS operates normally		
Check that there is adequate standby battery capacity to meet the requirements of current standards		
Check the operation of all WDs on system activation and when the hold-off voltage is removed from any self-powered device		
Check the operation of all tamper devices		
Check the area or volume of coverage of movement/vibration detectors including alignment of active beam detectors and any anti-masking or range reduction facilities (as appropriate)		
Check the entry/exit route(s) for correct operation and record entry/exit times		
Set system. Operate detection device(s) to check the resulting alarm condition(s) are notified correctly		
Test correct operation of all ATS paths (where fitted) for correct receipt of signals at the ARC		
If remote system checks or remote support is to be used, check correct synchronization of site specific parameters between I&HAS and secure computer		
Show the customer the extent of the detection coverage and correct operation of the I&HAS including the operation of detectors and the use of HDs		
Check that all documentation is correctly completed and customer documentation is left on site. Communication procedures with the ARC (if any) should be explained		
Obtain customer signature acknowledging receipt and correct operation of key/codes to the I&HAS		
Check that all surplus materials are removed from site and the premises left in a tidy condition		

The table is a suggested template for use. Other methods of recording the information may be used (provided the same information is recorded). Create a wider “remarks” column to enable enough information to be recorded.

6 PREVENTATIVE MAINTENANCE

6.1 General

Alarm company personnel must report faults to the client/user as soon as practicable.

Where faults are discovered during preventative maintenance, the alarm company must correct them. Where this is not possible (for example due to a shortage of replacement components) the alarm company must correct the faults as soon as practicable by taking prior agreed corrective action.

The reference to prior agreed corrective action implies that there is an agreement between the alarm company and the client detailing what needs to happen if a fault cannot be corrected during a preventative maintenance visit. Normally the details of such action will be included in the terms and conditions of the maintenance contract.

6.2 On-site preventative maintenance

Where possible, all parts of the I&HAS must be fully tested.

Parts of the system that cannot be fully tested must be recorded on the maintenance record, together with the reasons for their omission and the signature of the client or representative.

A record of checks and work carried out must either be given to the client at the time of maintenance visit or provided to the client within 10 days of the visit.

The record of checks may be in electronic form if this is acceptable to the client.

On-site preventative maintenance must meet Annex B.2 of the DD. This includes inspecting and testing the items in Table 4 below:

Table 4 – On-site preventative maintenance checks

Inspect and test the following are correct:	**Checked**	**Remarks**
The I&HAS meets the as-fitted document		
Tamper detection		
Setting and unsetting		
Entry and exit procedures		
Power supplies, including any alternative power source		
Functioning of detectors and hold-up devices		
Environmental conditions for adverse effects		
Operation of warning devices		
Operation of alarm transmission systems (all paths)		
Visual inspection for potential problems (electrical and physical)		
I&HAS equipment properly reinstated (put back into full working order) after testing.		

Create a wider “remarks” column to enable enough information to be recorded.

6.3 Remote system checks

Remote system checks must include those detailed in Annex B.3 of the DD and must also meet the specific details itemized in sub-clause 6.3.2 of the DD.

Table 5 below summarizes the position regarding remote system checks.

Table 5 – Remote system checks

Remote system check	Application of the check as per 6.3.2 of the DD
Interrogate event record and take appropriate corrective action (corrective action might require a site visit)	At least 40 events of the I&HAS event record must be reviewed. Any fault(s) found, or evidence that the system is not setting/ unsetting correctly, must be reported to the client/user.
Check the system has been set and unset (checks of setting and unsetting may be taken from event record)	No more specific details.
Check no adverse tamper or fault conditions exist on the system	No more specific details.
Check any alarm circuits that are on soak test	If any detectors are on soak test and there is no prior agreement with the client/user for the detectors to be on soak test, then: • either the client/user must be informed; or • action that has been generally agreed with the client for these circumstances must be taken *Detectors are not normally on soak test for more than 14 days.*
Check any alarm circuits that are inhibited/isolated	No more specific details.
Ensure time and date of clock are correct, update if required	The CIE clock must be checked for the correct date and time, and adjusted if necessary.
Check PPS is available	The client/user must be informed of any PPS faults that are found.
Check health of any APS	The remote system check must identify that the APS is charging (if applicable to the circumstances) and that the APS is capable of powering the I&HAS if a PPS failure occurs. The client/user must be informed of any APS faults that are found.
Check that “frequently used” detectors are operating	There must be a written agreement with the client detailing the “frequently used” detectors and the “non-frequently used” detectors. This agreement can be included in the as-fitted document. Subsequent changes to the “frequently used” detectors must be managed in accordance with sub-clause 8.1 of the DD. *Where an I&HAS has a limited number of “frequently used” detectors it may be more appropriate to consider on-site maintenance in preference to remote checks.*
Check correct operation of ATS (all transmission paths)	All transmission paths must be tested. The testing needs to be done in conjunction with the Alarm Receiving Centre (ARC), for example by using ARC logs to verify correct receipt of test signals.

There needs to be a written agreement with the client detailing the frequency of remote system checks (see Table 6 below for when remote system checks apply).

Confirmation that remote system checks have been carried out must be given to the client within 10 days of carrying out the checks.

The record of remote system checks may be in electronic form if acceptable to the client.

Remote system checks must not generate any false alarms.

If the remote system checks are carried out whilst the I&HAS is set, or any part of the I&HAS is set, the set parts of the I&HAS must remain set and continue to function normally.

A dialogue (see definition 3.1.6) for remote system checks must not prevent sub-clause 8.9.2 of BS EN 50131-1:2006+A1:2009 being met.

This means that during remote system checks the control and indicating equipment must notify any real intruder, hold up, tamper and fault signals to warning devices and alarm transmission systems within 10 seconds as per the standard.

A dialogue for remote system checks must not prevent BS EN 50136-1-1 being met.

This means that alarm transmission systems must continue to function normally during remote system checks and meet the alarm transmission system standard.

6.4 Frequency of preventative maintenance

The frequency of preventative maintenance must be in accordance with the DD. This is shown in Table 6 below.

Table 6 – Minimum frequency of preventative maintenance

Grade	**Number of visits**
BS 4737, BS 6799 WD only	one site visit per year
BS 4737, BS 6799 remote signalling	two site visits per year OR one site visit plus one remote system check per year A)
BS 7042	two site visits per year OR one site visit plus one remote system check per year A)
BS EN 50131 (PD 6662), Grade 1A, Grade 1B, Grade 1C and Grade 1T B)	one site visit per year OR a site visit every two years and a remote system check in intermediate years A)
BS EN 50131 (PD 6662), Grade 2X B)	one site visit per year
BS EN 50131 (PD 6662), Grade 2A, Grade 2B, Grade 2C and Grade 2D	two site visits per year OR one site visit plus one remote system check per year A)
BS EN 50131 (PD 6662), Grade 3A, Grade 3B, Grade 3C and Grade 3D	two site visits per year OR one site visit plus one remote system check per year A)
BS EN 50131 (PD 6662), Grade 4A, Grade 4B, Grade 4C and Grade 4D	two site visits per year
A) Substitution of one site visit per year with a remote system check is permitted only if the equipment permits all the relevant requirements of the DD to be met. B) Grades 1A, 1B, 1C, 1T and 2X are not suitable for police calling systems.	

Preventative maintenance must take place during the sixth calendar month (twelfth calendar month for annual visits) following the month of commissioning or following the month of the previous preventative maintenance visit.

Preventative maintenance carried out during the calendar month immediately prior to or after the due month, may be regarded as having been carried out on time.

Late preventative maintenance must not be used as the basis for scheduling subsequent preventative maintenance.

7 CORRECTIVE MAINTENANCE

An emergency service/corrective maintenance facility must be available to the client/user at all times.

The client must be given the contact details of the alarm company's emergency service facility.

The emergency service facility must be located and organized so that the alarm company's representative can attend the supervised premises as soon as practicable but at least within 4 hours or before the I&HAS is required to be set, whichever is the longer.

This period (of 4 hours) may be extended with installations on off-shore islands and those with local audible alarms only. The extended period must be agreed in writing by the client and subject to the approval of any insurer involved. The period may also be extended at the client's request, which needs to be recorded (by the alarm company).

8 REMOTE SUPPORT

8.1 General

Specific approval/agreement must be obtained from the client to apply remote support.

A dialogue (see definition 3.1.6) for remote support must not prevent sub-clause 8.9.2 of BS EN 50131-1:2006+A1:2009 being met.

This means that during remote support the control and indicating equipment must notify any real intruder, hold up, tamper and fault signals (if any) to warning devices and alarm transmission systems within 10 seconds as per the standard.

A dialogue for remote support must not prevent BS EN 50136-1-1 being met.

This means that alarm transmission systems must continue to function normally during remote support and meet the alarm transmission system standard.

The client/user must agree any change to an I&HAS that is implemented remotely, at the time of the change by prior arrangement.

This means that there must be a prior arrangement between the alarm company and the client (preferably in writing) to:

- *allow changes to be implemented remotely*
- *detail the way in which the client/user agrees to any change*

The alarm company must:

- maintain a record of all changes implemented remotely
- make the record available to the client as required

8.2 Use of remote support functionality

The use of all remote support functions by the alarm company (or ARC under contract to the alarm company) is subject to agreement between the client and the alarm company and (where applicable) the insurer. Remote support functions are subject to the conditions/ restrictions detailed in Table 7 below.

Use of all remote support functions is subject to the access level requirements of Table 2 of BS EN 50131-1:2006+A1:2009 (level 1, level 2, level 3, level 4 and so on).

Only those functions that may be used by the client/user when operating the I&HAS at the supervised premises can be made available to the client/user remotely.

Table 7 – Remote support functions

Function	Conditions/restrictions
Set or unset I&HAS (or part thereof)	By alarm company or ARC but only at specific request of client/user
Perform restore remotely	In accordance with BS EN 50131-1 and BS 8473
Change other site specific parameter	Not whilst I&HAS (or relevant part) is set
Apply or remove inhibit to alarm point or I&HAS function	With permission of client/user but not whilst I&HAS (or relevant part) is set
Apply or remove isolation to alarm point or I&HAS function	With permission of client/user but not whilst I&HAS (or relevant part) is set
Apply or remove soak test to alarm point	With permission of client/user but not whilst I&HAS (or relevant part) is set
Test warning device	With permission of client/user but not whilst I&HAS (or relevant part) is set
Activate or silence warning device	By alarm company or ARC but only at specific request of client/user

It is not mandatory to provide all of the remote support functions shown in the above Table.

9 DOCUMENTATION, AUDIT TRAIL AND RECORDS

Records of all maintenances, temporary disconnections and remote support carried out, and of any corrective measures taken or required, must be made and retained for a minimum period of 15 months after the site visit, remote system check or remote support to which it refers, so that a full audit trail is available of work performed at site and from each secure computer. The records must include:

- date and time
- detailed records of the checks undertaken and the results
- details of any changes made to system configuration
- identity of personnel carrying out the work
- identification of the secure computer used in any dialogue
- details of any temporary disconnection including date time and reason for the disconnection and subsequent reconnection
- identity of the client/user authorizing such changes/disconnections

****