integration of intruder alarm systems

with other systems under PD 6662 – a guide

July 2013

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

Image©istockphoto.com/IDFK303

Form No. 169 Issue 1

Contents

Introduction

In the UK the requirements related to installation of Intruder and Hold-up Alarm Systems (I&HAS) are given in a series of standards covered by a scheme numbered PD 6662 and published by BSI. The primary standards included under this scheme are the European Standards in the BS EN 50131 series and a number of additional British Standards such as BS 8243. These standards are written on the basis of a system comprising a collection of parts that are all specifically intended to be parts of an I&HAS.

In some cases systems may be installed where parts of the I&HAS are integrated with other systems. An example of this integration may be an I&HAS with a home automation or building management system. In these examples the customer may wish for the other system to provide a user interface that can control the I&HAS. So that the I&HAS may meet the requirements given by PD 6662 the standards need to be applied appropriately. The purpose of this document is to give guidance related to the areas of the standards that relate to integrated systems.

1. Scope

This document gives guidance for the application of the standards for intruder and hold-up alarm systems to integrated systems. An integrated system in this context is one that includes an intruder and hold-up alarm system (I&HAS) and some other system whether that be a security related system (e.g. access control), a fire detection system, a building management system, home automation system or some other equipment.

This guide mentions grade 1 and grade 4 I&HAS but does not include specific guidance related to these systems.

2. Terms, definitions and abbreviations

2.1 Definitions

2.1.1 Remote Location

EN 50131-1 refers to "remote location" as a possible place for the storage of the event record in clause 8.10.

Note 1: This term is not precisely defined and it could be argued that event records kept by an integrated system could be covered by the term "remote location". The access to the event log should still be restricted according to the access level of the user (see 4.2).

Note 2: DD 263 defines a remote location as "premises of an alarm company or ARC from where it is possible to initiate and/or process remote system checks or remote support". This definition is only relevant in the context of the requirements of DD 263.

2.1.2 Virtual Keypad

A method of achieving user control of an I&HAS through a different interface that replicates the appearance of the I&HAS keypad (e.g. by showing a representation of the I&HAS keypad on a touch screen).

Note: The implication of this type of interface is that the system providing the virtual keypad simply passes the keystrokes to the I&HAS and is not aware of the meaning of the actions. For example the entering of a four-digit PIN would not be recognised as a code but simply four digits and therefore the system could not use this information to record the user identity.

2.2 Abbreviations

ACE Ancillary Control Equipment (A device that controls the I&HAS, e.g. keypad)
ACS Access Control System
ARC Alarm Recieving Centre (also known as "a monitoring centre")
CCTV Closed-Circuit Television
HA Hold-up Alarm
HAS Hold-up Alarm System
I&HAS Intruder and Hold-up Alarm System
IAS Intruder Alarm System

3. Fundamental Aspects

3.1 When does a system need to comply with PD 6662?

An intruder and hold-up alarm system (I&HAS) needs to comply with PD 6662 when:

a) The system transmits alarms to an Alarm Receiving Centre (ARC) for the purposes of gaining police response to alarms. When this is done the I&HAS requires a Unique Reference Number (URN) from the police. This is the normal method of obtaining police response to automated alarms. It is very rare to have a direct connection to the police.

b) The system needs to have a certificate issued by an inspectorate. This is a requirement for obtaining police response but can also be a requirement from insurance companies. For an installation company to be able to install certificated systems they must also be audited by the inspectorate and this implies that the systems they install must comply with PD 6662 scheme requirements even if this is not needed for police or insurance needs.

3.2 What is PD 6662?

PD 6662 is the number of a scheme document published by British Standards that details a number of standards that should be used together to achieve compliance as described above. The scheme includes standards for the system, its installation and maintenance and the components that make up the system. The primary standards that affect system design and installation are BS EN 50131-1, DD CLC/TS 50131-7, and BS 8243.

BS 8243 is the standard that defines the method by which alarms are considered to be "confirmed". With regard to intruder alarms normally only confirmed alarm signals can cause a request for police response. For hold-up alarm systems confirmed signals may be required in some circumstances. Note that it is the signal that is "confirmed" not the system. Compliance with the requirements of BS 8243 is necessary only if the I&HAS is intended to gain police response to alarms.

3.3 What is the Security Grade?

The Security Grade is a measure of the resilience of the I&HAS to outside influences and to attack by criminals. There are four grades with grade 4 being the highest. However grade 4 systems are for practical purposes non-existent. Only grade 2 and 3 systems can gain police response to alarms. The UK has two specific types of system "1T" (Grade 1 option T, which is for low risk situations) and "2X" (Grade 2 option X, which does not have signalling to an ARC). Neither of these options is permitted to have police response.

3.4 What is the Environmental Class?

In addition to the security grade there is also an environmental classification. This is used to ensure that equipment is suitable for its location according to temperature, exposure to damp, tolerance to vibration and shock, etc. The classifications are:

- Environmental Class I: Indoor ($+5^{o}$ to $+40^{o}$)
- Environmental Class II: Indoor General (-10^{o} to $+40^{o}$)
- Environmental Class III: Outdoor Sheltered or Indoor Extreme (-25^{o} to $+50^{o}$)
- Environmental Class IV: Outdoor General (-25^{o} to $+60^{o}$)

3.5 Separation of Systems

It is recommended that to assist with a claim of meeting the requirements of PD 6662 integrated systems be designed with a clear definition of the boundary of the systems. Additionally the ability to demonstrate that systems are independent (For example by provision of separate keypads that can enable independent operation and by not sharing power supplies) will assist with proving such claims. Where this is not possible without compromising the functionality of an integrated system then the recommendations of this guide should be followed.

3.6 Claims of Compliance

Clause 4 of PD 6662 gives requirements for claims of compliance.

Any item of equipment that has a relevant standard in the list in 3.2 of PD 6662 should meet the requirements of that standard if it forms part of the I&HAS. If a device is used that does not have a related standard then it should "be suitable". This means that it should meet the general requirements given in EN 50131-1. For example the necessary tamper detection requirements should be fulfilled. This could restrict the sharing of devices between the I&HAS and an integrated system.

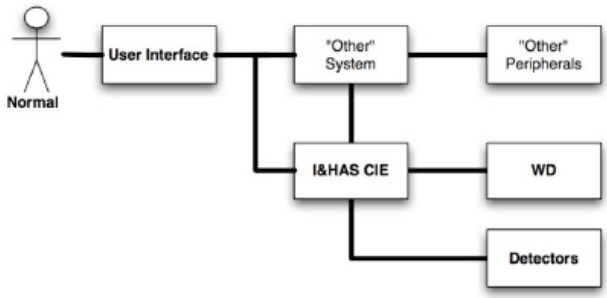
3.7 Categorisation of Integrated Systems

Depending on the arrangement of devices, level of integration and technology used for connecting components a variety of different types of integration are possible. For the purposes of making the description of requirements easier this document employs a categorisation of systems from the point of view of the I&HAS.

Type A

A user interface (e.g. keypad) for the integrated system allows the user full control of the I&HAS providing all of the functions required by EN 50131-1 and meeting all necessary component standards for ACE in EN 50131-3 whilst also acting as user interface for other systems. By definition the user interface is part of the I&HAS but it may also need to comply with requirements related to other systems.

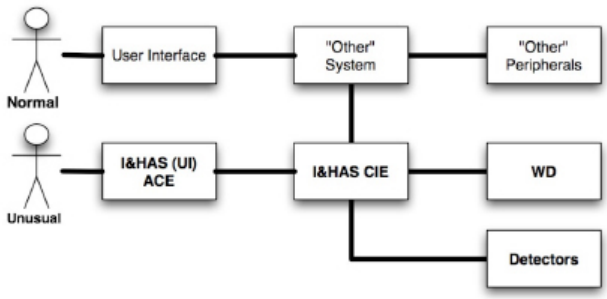
Example Type A System Arrangement:



Type B

A user interface (e.g. keypad) that is not part of the I&HAS provides day-to-day control of the I&HAS but an additional interface that is part of the I&HAS provides the EN 50131 related requirements and if necessary can allow normal I&HAS operation. The consequence of this is that this interface must be located in a suitable position to allow setting/unsetting of the system without causing alarm conditions.

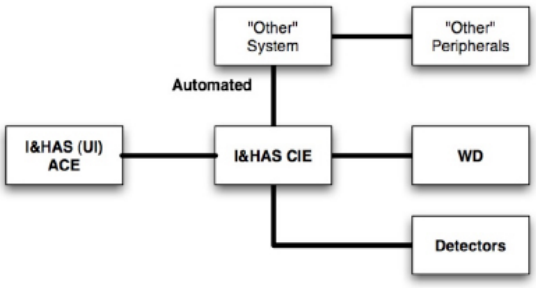
Example Type B System Arrangement:



Type C

The I&HAS is an independent system but is linked to another system that facilitates some automated features. For example: integration with an access control system that can determine whether the IAS should set or unset according to the people moving on/off site. With this type of system the user is not directly controlling the I&HAS; the other system is making decisions and affecting the I&HAS. If necessary the I&HAS can be manually operated independently of the other system(s).

Example Type C System Arrangement:



3.8 Cautions regarding shared use of components

Care should be taken when considering integration of components. Components that may on first sight appear to offer equivalent functionality often do not.

For example a movement detector intended to activate lighting or open a shop door may be overly sensitive (e.g. detecting movement outside of the intended area) because the consequences of accidental operation have little impact. Movement detectors for I&HAS include features intended to reduce the risk of false alarms. The two types are not interchangeable.

4. EN 50131-1 Requirements

4.1 Recommendations Regarding EN 50131-1 Requirements

The following table lists recommendations and gives information about the requirements of EN 50131-1 on a clause-by-clause basis. Where no recommendations are thought necessary the clause is not listed.

Table 1 - Guidance on EN 50131-1

Clause/Table	Subject	Guidance
4	System Functions	The clause lists the functions that are considered part of the I&HAS and, with relevance to integration, states that "additional functions" may be provided "providing they do not influence the correct operation of the mandatory functions." This means that it is permitted to have functions within the I&HAS that provide interfaces and transfer information to an integrated system. Care needs to be taken that this does not affect the requirements of the I&HAS given in the standard. It is to the benefit of meeting the standard to have a clear understanding of which parts of an integrated system constitute the I&HAS and which do not.
5	System Components	Those components that are considered to be part of the I&HAS must be classified for environmental classification (see clause 7) and given a Security Grading. In the absence of requirements for certification and/or third-party testing the provision of an environmental classification is relatively easy and could be adopted by equipment not originally intended for I&HAS. It is possible, but more difficult, to determine the security grading of such equipment. If it is intended to do the latter then the necessary component standard of the EN 50131 series should be applied if one exists and in other cases a requirement may be determined by analysis of the generic requirements of EN 50131-1 or other standards in the PD 6662 scheme.
6	Security Grading	See guidance on clause 5. The equipment to provide a security grade 4 I&HAS is not generally available. The highest grade is likely to be grade 3 (although some aspects may exceed the minimum requirements for grade 3). It is unlikely that the customer of an integrated system would wish to have a security grade 1 system. In the UK Grade 1 systems cannot be used to obtain police response to alarms and consequently tend to fall outside of the "professional" market category. This guide assumes that grade 1 systems will not be used.
7	Environmental Classification	See guidance on clause 5.
8	Functional Requirements	
8.1	Detection Functions	As with clause 4 (System Functions) this clause permits "other events" to be detected "providing this does not adversely influence the mandatory requirements".
8.1.2	Hold-up Device – Triggering	EN 50131-1 includes a requirement that "Hold-up devices shall include means to minimise the possibility of accidental triggering." The PD 6662 scheme (by way of BS 8243) and the ACPO policy (England, Wales and Northern Ireland) gives extra requirements for hold-up devices. These effectively mean that non-I&HAS specific devices should not be used to trigger hold-up alarms. (See 4.4 below for further details). In particular touch screen interfaces would not satisfy the UK requirements and neither would most keypads (unless specifically designed to meet the UK requirements).

Clause/Table	Subject	Guidance
8.1.3	Tamper Detection	Any component considered to be part of the I&HAS should incorporate the required tamper detection (see comments on clauses 8.7.1 to 8.7.4).
8.1.4 & Table 1	Recognition of Faults	Whilst this table makes it mandatory for the I&HAS to recognise certain faults it is not this table that makes it a requirement for components to signal such faults to the system. Component standards contain detailed requirements and other clauses within EN 50131-1 give some basic fault related requirements.
8.2	Other functions	This clause includes requirements for detection of masking of movement detectors in security grade 3 and 4 systems and for detector range reduction detection for grade 4 detectors. If a type of movement detector was to be employed in an integrated system that did not have a specific component standard within the EN 50131-2 series of standards then this generic requirement could affect the ability to claim compliance with EN 50131-1 at grades 3 and 4. An example of such a movement detector could be detection derived from video analysis of the image from a CCTV camera in an integrated CCTV and intrusion system.
8.3	Operation	The requirements for controls to be clear, unambiguous and logically arranged may be subjective and difficult to prove but use of a system that obviously disregards this could result in failure of the system to meet the standard.
8.3.1	Access Levels	The requirements related to access levels and the related user authorisation requirements are fundamental to the security of the I&HAS. For the avoidance of ambiguity refer to 4.2 (below) for further details about the differences between access levels. Note that the method (b) of achieving authorisation to access the system at access level 3 is not typically used in the UK.
Table 2	Levels of Access	This table gives requirements restricting the functions that users at different access levels (see 4.2) are permitted access to. If the access to the I&HAS is made via an interface to a non-I&HAS part of an integrated system then restrictions of access should comply with this table. This may cause difficulties because of incompatibilities. A discussion of these problems is given in 4.3
8.3.2	Authorisation	The stated requirements of EN 50131-1 are restricted to "logical keys" (e.g. PIN codes, passwords, stored data in token/badge etc) and "mechanical keys" (e.g. a traditional shaped metal key). If either of these methods of authorisation are permitted to gain access to the control of the I&HAS then the requirements apply. For example, for a Grade 3 I&HAS a PIN must have 100,000 differs (such as a five digit number, 00000 to 99999).
8.3.3	Setting and Unsetting	Providing the appropriate authorisation has been used to obtain access at the correct access level (i.e. access level 2 or 3) this should not represent a problem to an integrated system.
8.3.4	Setting	See guidance on clause 8.3.3 and the comment about security grade 1 systems in the guidance to clause 6. Care should be taken with regard to unsetting options in BS 8243 (6.4.5, etc) and audible indications.

Clause/Table	Subject	Guidance
8.3.5	Prevention of Setting	The user needs to be aware that the system cannot set and the exact reason needs to be available from at least one I&HAS interface but not necessarily from other devices. In the event that one of the conditions given in this clause should prevent setting then two options would be available to an integrated system according to its type. Type A: The user interface can fully control the I&HAS. Type B and Type C: The user can bypass the user interface that they normally use and operate the I&HAS from an alternative interface that forms part of the I&HAS. In this case care needs to be taken that this alternative interface is located so as to avoid causing other faults or false alarms when trying to set the system.
8.3.6	Overriding Prevention of Setting	See guidance on 8.3.5. Also see guidance on 8.3.1 to understand the difference between access level 2 and 3.
8.3.7	Set State	It is recommended that the option given under c) is not used. It is not permitted under BS 8243. Option c) implies that only an indication is used to show that entering an area will cause an alarm. Be aware that this restriction applies to any system that can transmit an alarm e.g. it would apply to a door leading from an unset living area into a garage where the alarm was set. For an integrated system opportunities may exist to use option “a)”.
8.3.8	Unsetting	For an integrated system opportunities may exist to avoid the use of an entry route (the route from the entrance to the user interface) by linking the I&HAS to a form of access control. If an entry route is required the procedures required for unsetting would require that in all circumstances the point of unsetting (e.g. proximity reader) should be close to the door so that it can be operated within 45s. This would also apply to an alternative interface (e.g. if this was a Type B or C system). It is also recommended to keep this entry route short because generating a confirmed alarm from this part of the premises is less likely.
8.3.9	Restoring	See guidance on 8.3.1 to understand the difference between access level 2 and 3. Restoring requires knowledge about the condition and history of the system and so the requirements of 8.5 and in particular 8.5.3 are relevant.
8.3.10	Inhibit	Inhibiting is the removal of a function (e.g. a detector) until the next time the I&HAS is unset (i.e. it is automatically reactivated). See guidance on 8.3.1 to understand the difference between access level 2 and 3.
8.3.11	Isolate	Isolating is the removal of a function (e.g. a detector) until a user reactivates it. See guidance on 8.3.1 to understand the difference between access level 2 and 3.

Clause/Table	Subject	Guidance
8.3.12	Test	Typically this is a "walk-test". The I&HAS will indicate that a detector has been activated but there is normally a need to view a display for confirmation of this.
8.3.13	Other Functions	This clause specifically allows for integration but requires that operations that can affect the I&HAS are restricted by user type.
8.4	Processing	Integration should not affect this.
8.5	Indications	Three types of indication are described. 1) Those marked M in table 9 must be available to all persons (whether users or not). 2) Those marked NP in table 9 must not be available to anybody unless they have identified themselves to the I&HAS (i.e. access level 2, 3 or 4). 3) Those marked M in table 8 must be available to access level 2, 3 or 4 users. Additionally they must all be visible at a single location. This could be a specific interface point used for that purpose.
8.5.3	Cancelling Indications	This does not mean that the information stays on the display continuously. If there has been no user activity then the indication mandated by table 8 should be cleared (and probably replaced by any mandated information from table 9).
8.6	Notifications	Notifications consist of signals sent via an Alarm Transmission System (ATS) to an ARC and sound from a Warning Device (WD). Providing the methods of notification meet the requirements of table 10 (or Grade 1T or 2X, see 3.3) then other transmissions and sounds can be generated so long as they do not interfere. The choice is made from one of the options within each grade (e.g. Grade 3, option C). Insurance companies might request that the ATS rating is higher than that shown in table 10. The mandatory notification equipment must comply with the component standards listed in PD 6662. A variance to this applies to Grade 1T. For example if a system requires an audible WD to be fitted it should meet EN 50131-4 but that does not prevent the use of additional speakers to generate sound over a wider area.
8.7	Tamper Security	The requirements of this clause apply to the I&HAS and any components considered to be part of the I&HAS, whether or not they have a specifically associated component standard. Providing that other equipment used as part of the integrated system cannot adversely affect the I&HAS or control it, then these tamper requirements do not apply. Refer to table C.1 in Annex C of EN 50131-3.
8.8	Interconnections	Interconnections go from one component of an I&HAS to another. They do not include cables and signals leaving the I&HAS (e.g. to go the ARC). Interconnections can be shared with other systems (see 8.8.2) providing the availability of the interconnection to the I&HAS is sufficient for its functioning (e.g. a shared IP type system should have sufficient bandwidth or limits on use of the bandwidth so that the I&HAS continues to work as normal). See also Annex C of EN 50131-3.

Clause/Table	Subject	Guidance
8.9	I&HAS timing performance	Integration should not affect this
8.10	Event Recording	The event log described is a function of the I&HAS. If integration is by use of a "virtual keypad" (see definitions) arrangement then there may be issues about logging the necessary information. Whether this is a problem depends on the exact method of operation and the functions being performed. In the majority of cases an event is likely to be logged when a virtual keypad is used but in some cases the integration may be achieved by unorthodox means that by-passes the normal processes. Care should be taken to ensure the method of use meets the requirements. It may be possible to apply the permission to store the event log at a "remote location" (see definitions) to an integrated system.
9	Power Supply	Any equipment needed to operate the I&HAS should be powered so that these requirements are met. If a type B or type C integration is used then the I&HAS ACE should be located in a place suitable for its use. Note that the standby time required under PD 6662 is reduced from that stated in EN 50131-1, table 23, Type A (it is typically 12 hours at all grades). If the non-I&HAS system is necessary to operate the I&HAS then there should be signalling of power fail faults to the I&HAS. If the non-I&HAS is not needed to operate the I&HAS then there are no relevant power supply requirements (see Annex C of EN 50131-3, see 5)
10	Operational Reliability	These requirements would apply to the user interface for an integrated system.
11	Functional Reliability	The use of an integrated system should not affect the functional reliability of the I&HAS.
12	Environmental Requirements	The integration of the I&HAS with other systems should not affect the I&HAS from an environmental perspective. In particular there should not be any EMC interference.
13	Electrical Safety	Good electrical installation practice should seek to avoid problems
14	Documentation	Any required documentation for the integrated system that might affect any of these items should be supplied (e.g. amended operating instructions)
15	Marking / Identification	Integration should not affect this

4.2 Access Levels

Access Level is the term given to the level of authority that a person has over the I&HAS. Four access levels are described and particular care is required with the meaning of access level 3.

Access Level	User Description
1	Not known to system. e.g. a member of the public or a user that has not identified themselves. Information available to an access level 1 user is freely available to anybody.
2	A typical end-user or one with limited access to set/unset the system
3	An end-user "supervisor" such as a person with authority to create new end-users (Note this is a typical interpretation but this user could be at access level 2).
	An installer / engineer with permission to make changes to the system affecting its design or to carry out maintenance.
4	The manufacturer gaining access without physically contacting the system (i.e. by remote access).

Although Table 2 in EN 50131-1 describes the relationship between system functions and access level it gives permissions rather than mandatory abilities. Each individual user can be configured to have a restricted range of functions. For example the "supervisor" described above would not have the ability to "add/change site specific data".

4.3 User Authorisation by non-I&HAS interface

If the identification and granting of authorisation is performed by the I&HAS then compliance with PD 6662 is simpler. For compliance with Annex C of EN 50131-3 (see 5) initiation of communication between the I&HAS and non-I&HAS should be achieved with the same authentication EN 50131-1, clause 8.3.2 (although this could be achieved by using the authentication to gain access to the non-I&HAS user interface or the security related subset of that interface).

4.4 Hold-up Devices (PA Buttons)

A hold-up device, commonly known as a "PA" (panic alarm) is a fixed or portable device used to call for an emergency response when a user is under threat. PD 6662 requires that such devices conform to BS 4737-3.14: 1986 clause 3.2b) or 3.2c). This means that "two forces" of between 4N and 5N must be applied either simultaneously or consecutively. In practice this means two separate mechanical buttons. This typically rules out the use of touch screen devices.

In the majority of cases hold-up devices will be used to gain police response and therefore need to meet the additional requirements of BS 8243: 2010, clause 4.5. This in turn means that the buttons used for the hold-up device cannot be used for other purposes (i.e. using two numeric keys on a keypad is not permitted).

***Note**: Police forces are seeking to reduce the number of false alarms. Many of these can be attributed to misuse rather than accidental use. Causing an excessive number of false alarms (e.g. two per year) may lead to a loss of police response and subsequent imposition of additional restrictions and procedural changes.*

5. EN 50131-3 Requirements

5.1 Annex C – Introduction

Annex C of EN 50131-3 contains normative requirements for the use of "non-I&HAS interface" and would therefore appear applicable to the integration of systems where the interface provided to the user is by way of the other system (i.e. a Type B integration). The details given in Annex C are listed in Table C.1 and either impose additional requirements or relax those given elsewhere. The requirements apply to:

a) Communication Software Protocols
b) The non-I&HAS interface and connections thereto

5.2 Table C.1 – Application to Integrated System

The following table repeats the contents of Table C.1 in EN 50131-3 but with additional guidance. Note that the Clause number indicated in the table is not consistently the clause in EN 50131-3 (and is sometimes EN 50131-1 as noted below).

The major issue is the monitoring of substitution of the non-I&HAS interface by the I&HAS.

Table 2 - Guidance on EN 50131-3 Table C.1

Clause	Title	EN 50131-3 Requirement	Guidance
7	Environmental	Not Applicable	
8.3.2	Authorisation	Access to the communications software at the non-I&HAS interface shall comply with this requirement.	See Table 1, 8.3.2 of this guidance.
	Authentication	Initiation of communication between the non-I&HAS interface and the I&HAS shall have authentication equivalent to the requirements of 8.3.2	This requirement applies the user authentication to the initiation of communication (although this could be achieved by using the authentication to gain access to the non-I&HAS user interface or the security related subset of that interface).
8.5.1	Indications	Indications at the non-I&HAS interface may be considered as equivalent to a mimic panel (see 8.5.1 Note 2).	This implies that either the indications conform to the requirements in EN 50131-1 or that they are normally hidden from view (e.g. by being inside a security room or a locked cabinet).
8.7.1	Tamper Protection	Not applicable	
8.7.2	Tamper Detection	Not applicable	
8.7.3	Monitoring of Substitution	The requirement shall apply at all grades [a]	The requirements in 8.7.3 apply normally only to Grade 4. This implies that the requirement for grade 4 applies to all grades but with the timing of 100s (see table 15 in EN 50131-1) for grades 1, 2 and 3. This probably means the use of a serial interconnection. The requirement in EN 50131-1 applies to components (not interconnections).
8.7.3	Timing requirements	The grade 3 requirement shall apply additionally at grades 1 and 2 [a]	

Clause	Title	EN 50131-3 Requirement	Guidance
8.8	Monitoring of Interconnections	The requirement of 8.8.3 (Table 16) is not applicable to portable devices.	The reference to 8.8.3 and Table 16 is to EN 50131-1. No additional requirements appear to apply to non-I&HAS interfaces.
8.8	Security of Communication	The requirement of EN 50131-1: 2006, 8.8.5 (Table 19) shall apply at all grades.	The requirements in 8.8.5 apply normally only to Grade 4. This implies that the requirement to detect delay, modification and substitution of messages applies to the non-I&HAS interface at all grades.
8.11	Power Supply	The requirement of EN 50131-1: 2006, 9.2 for APS is not applicable.	No related requirements apply to non-I&HAS interfaces.
[a] If the device does not include the capability to provide input to the I&HAS, this requirement is not applicable.			

6. BS 8243 Requirements

6.1 Recommendations Regarding BS 8243 Requirements

BS 8243 is a standard for confirmation of alarms. The use of alarm confirmation is intended to reduce the number of alarms that result in the use of police resource. Alarms that have not been confirmed (unconfirmed alarms) usually result in a call by the ARC to the key-holder.

The standard attempts to address a number of areas identified as causing false alarms and placing restrictions on system design to avoid these. It then describes methods by which alarms can be confirmed.

The following table lists recommendations and gives information about the requirements of BS 8243 on a clause-by-clause basis. Where no recommendations are thought necessary the clause is not listed. There is no discussion here of the design of the installation to achieve suitable confirmation. The guidance given here relates only to the integration of I&HAS with other systems.

Table 3 - Guidance about BS 8243 requirements

Clause	Title	Guidance
1	Scope	BS 8243 contains requirements for confirmation of intrusion signals and for hold-up alarms. The use of BS 8243 is mandated only if signals are sent from the I&HAS with an intention to gain police response. The application of BS 8243 to hold-up alarm confirmation is mandated only if required by the police.
4.2	Alarm Confirmation Technology	IAS must use "sequential confirmation technology" and may use "audio" or "visual" confirmation. HAS (when applicable) must use one or more of: "sequential confirmation technology", "audio", "visual" or "telephone" confirmation (call-back). The telephone confirmation method is a procedural matter and is not affected by integration.
4.5	HAS confirmation	See 4.4 of this document (above).
5.1.3	Control and Indicating Equipment (CIE) and Notification Equipment	The "CIE" includes the I&HAS control unit ("control panel"), keypads or readers. It is recommended that any integrated system components that could influence the I&HAS are located according to this clause.

Clause	Title	Guidance
5.2	Audio Confirmation	If audio confirmation is to be used then there is a need to avoid creating sounds that would interfere with the ability to hear what is happening on the site. If the audio confirmation is to use part of the integrated system (e.g. via microphones possibly also used for other purposes) then they would need to operate and be used in compliance with BS 8243 requirements.
5.3	Video Confirmation	If video confirmation is to be used then there is a need to avoid the creation of lighting influences (e.g. strobes) that would interfere with the ability to see what is happening on the site. It is recommended that any video technology is specifically intended for the I&HAS to ensure it can be used effectively (e.g. by matching coverage areas with detector coverage).
6.3	Methods of completion of setting	The use of an integrated system could suggest to the installer or customer that a convenient solution might be used for the setting of the alarm system. For example, an access control system (using type C integration) could determine that the building was no longer occupied and automatically cause the I&HAS to set when the last person leaves. This is NOT PERMITTED by BS 8243. The methods allowed for setting the system are given in this clause together with a requirement that (unless the ARC sets the system remotely) then setting of the system must be a "two-stage" process. This means that the user must start the setting process from inside the premises and then one of the described methods used to complete the setting. ***Note:*** *The requirement for two-stage setting process is likely to be removed from BS 8243 in its first amendment.* During the time between the user starting the setting process and the completion of setting there should be an audible indication of setting. It should be possible for the user to tell that the system has set.
6.4	Methods of unsetting	Only the methods described are permitted. It is strongly recommended that method 6.4.4 is not used. The use of an integrated system could lead to the use of methods 6.4.2 or 6.4.3 and these would be recommended. The commonest method used in the intruder alarm industry is 6.4.5
6.4.5	Completion of unsetting using a digital key	A digital key is typically a proximity token or badge, key fob, etc. The method of operation should not use a PIN code. The use of the PIN is only permitted when the entry timer has expired and the system is in alarm. The important phrase to note is "unsetting is achieved by a single manual action using a digital key". This prevents the use of fob and code combinations. See also the guidance on EN 50131-1, clause 8.3.8
7.1.1	Listening-in	Note the requirements restricting when listening-in can be used. Any conflict of this requirement with parts of an integrated system should be considered.
7.2.1	Viewing	Note the requirements restricting when images can be viewed. Any conflict of this requirement with parts of an integrated system should be considered.
Annex A.1	Tamper Detection	The audio or video confirmation devices (microphones, cameras, etc) should include tamper detection matching those required by EN 50131-1 at the grade specified (see tables 12 and 13). This requirement would affect devices forming part of the integrated system.

Worcester

Kirkham House
John Comyn Drive
Worcester
Worcestershire
WR3 7NS

London

Market House
85 Cowcross Street
Farringdon, Islington
London
EC1M 6PF

tel +44 (0)845 389 3889
fax + 44 (0)845 389 0761

info@bsia.co.uk
www.bsia.co.uk

@thebsia