PROTECTOR

Intrusion and Hold-up Alarm Systems

Introduction

British Standards for intruder alarm systems were replaced in favour of a harmonised European Standard on 1st October 2005.

British Standards which have been replaced are:

- BS4737: Intruder Alarms Systems: specification for installed systems with local audible and/or remote signalling.
- BS6799: Code of Practice for wire-free intruder alarm systems.
- BS7042: Specification for high security intruder alarm systems in buildings.

All new intruder alarm installations must be designed and installed to the new European Standard (EN 50131 / PD 6662).

Existing intruder alarm systems and upgrades to existing systems will still be subject to British Standards applying at the time of their installation; but exceptionally may need to comply with European Standards if they require such extensive re-design/equipment replacement that they effectively become a 'new system'.

Implementation

Because not all the relevant European Standards have been published and the Euro Standards do not cover some issues that alarm systems may be required to meet in the UK to satisfy the Police and Insurers, The British Standards Institute have published an "enabling standard":

- PD 6662: 2017: Scheme document for the application of European Standards for Intruder and Hold up Alarm Systems.

This will enable the published European Standards and mature draft standards to be introduced in a controlled and consistent way across the industry. It will enable end users, insurance companies and others to specify, and security companies to install, intruder alarm and hold-up systems to European Standards.

All risk improvements made for clients to install a new intruder alarm system should quote "in accordance with the scheme described under PD6662: 2017" and not EN 50131.

Note: the Scheme applies to conventional (hard-wired) intruder alarm systems as well as wire-free intruder and hold-up alarm systems in buildings. The Scheme does not apply to exterior intruder alarm systems or deterrent systems which should continue to be installed in accordance with current British Standards.

There are several key differences between the old British Standards and the new European Standards:-

Risk Assessment

Installers are required to carry out a formal risk assessment to determine a suitable Grade and design of the system.

The adoption of a risk assessment approach should lead to a better designed system that is commensurate with the risk and meets the customers and insurer's needs.

The European Standard document DD CLC/TS 50131-7: Alarm systems – Intrusion systems: Part 7: Application Guidelines provides guidance to installers on a grade by grade basis on the likely possible points of intrusion that should be considered when designing a system and also requires installers to undertake and record a risk assessment before designing the system.

The Application Guidelines include Annex A (Contents) and Annex B (Buildings) which emphasise factors and areas that should be considered:

Annex A: Contents	**Annex B: Buildings**
The design of the system should be consistent with the risk of an attack on the protected premises. The level of risk will be dependent, among others issues, on the type of contents. Examples of issues that should be considered are:-	When considering the element of risk in the design of an intruder alarm system the structure of the premises to be protected will be a major determining factor. Examples of issues that should be considered are:-
Type of contents Value Bulk or size Theft history Danger Damage	**Construction** Openings (doors, windows, rooflights) Occupancy Keyholding Locality Existing security Theft history Local legislation or regulation

There is no requirement in the European Standards for the risk assessment to be shown to the customer or their insurer, but some installers may choose to enclose a copy of the risk assessment with the alarm specification.

System Grading

The principle of Grading systems in terms of their security provision and the extent of the detection the system provides into four Grades (with Grade 1 being the lowest), based on the anticipated level of skills/knowledge, resources (e.g. tools) and determination shown by intruders at each level of risk.

Grade	**Risk**
1	Low risk / little knowledge / limited tools
2	Low to medium risk / limited knowledge / some tools
3	Medium to high risk / some knowledge / full range of tools

4 High risk where security takes precedent over all other factors / good knowledge / sophisticated tools.

These Grades are based on operational requirements concerning matters such as resistance to compromise, performance and resilience necessary to defend the protected premises against the expected severity of attack. They influence the design of all important components - detectors, control equipment, connections, power supply and signalling. Each piece of equipment must be marked with the Grade with which it complies and the overall Grade of the system is governed by the rating of the lowest graded component.

The following table highlights some of the differences between the Grades:-

Table 1. Comparison of security grade features

Feature	Security Grade			
	1	2	3	4
Signalling warning devices	Choice of audible warning device or low grade remote signalling	Warning device and remote signalling (2X permits audible only)	Warning device and enhanced remote signalling	Warning device and high security signalling
Movement detectors	Tamper detection optional	Tamper detection mandatory	As Grade 2 + anti-masking detection	As Grade 3 + range reduction detection
Level of supervision (guide to the method of intrusion to be considered)	Opening of external doors + trap	Opening of external doors and windows etc + trap	Opening of and penetration through external doors and windows etc + trap and special consideration to high risk items	As Grade 3 + penetration of walls, ceilings, roof and floor
Tamper	Control and indicating equipment + signalling equipment + warning devices + power supplies	As Grade 1 + detectors + junction boxes	As Grade 2 + anti-masking and adjustment of orientation of detectors	As Grade 3 + penetration of controls and signalling equipment + penetration of warning devices
Event recording	Not required	250 events	500 events + user ID	1000 events + user ID
Maintenance required per year – as required by	1 site visit	2 site visits OR 1 site visit + remote diagnostic check (Option 2X – audible only – 1 site visit)	As Grade 2	2 site visits

Grade 1 (very low standard, equivalent to D.I.Y.) - offers significantly lower protection than that required by BS 4737 and therefore is not acceptable to protect risks where an alarm is a requirement of insurance.

Grade 2 (Acceptable for low risk only) – similar to intruder alarms installed to BS 4737 but does not require certain features that have become expected in systems installed in the UK, such as 500 event memory log in the control panel, user identification in the memory and prevention of change of orientation of detectors (i.e. moving a detector when the system is unset to prevent detection when the system is set). Due to these shortcomings insurers should only accept Grade 2 systems for (i) most household risks and (ii) some low risk commercial premises.

Grade 2X - In addition, to Grades 1-4 of the European Standards PD6662:2010 introduces an extra Grade 2X to enable Grade 2 systems to be installed without remote signalling (i.e. attended risks).

Grade 3 (Acceptable for majority of risks) – provides a similar level of protection to that currently installed in the majority of commercial premises throughout the UK, but requires enhanced movement detectors that have the ability to determine that they have been 'masked' (i.e. the detector has been covered or sprayed to prevent operation). It does not require a detector to recognise a reduction in range (for example something blocking the field of detection but not actually on or extremely close to

the detector). Grade 3 is the grade of choice for intruder alarms in commercial premises and should be the safe default for installers uncertain of insurance requirements.

Grade 4 (High security risks) – equates to a high security system and is appropriate for commercial premises that would previously have justified the installation of a BS 7042 alarm. It is expected that very few Grade 4 systems will be required to be installed by insurers.

Note: *The European Standards give good guidance on the factors to consider when carrying out a risk assessment. However the choice of Grade is subjective and the Standards do not quantify exactly what is meant by low, medium and high risk. As the determination of Grade will largely be decided by the alarm installer Grade 2 type systems may be chosen in preference to Grade 3 due to competitive pressure. This could result in additional expense for clients if insurers get involved at a later date and require a system upgrade.*

Signalling (referred to in the new standards as Notification)

EN 50131 gives various 'Notification Options' (A, B, C, D or X – i.e. siren, siren plus single link to ARC, two links to ARC etc.) of 'Warning Device' (formally bells, sounders and sirens) and 'Alarm Transmission Systems' (remote signalling) permitted for each of the four Grades -

NOTIFICATION OPTION	MINIMUM REQUIREMENTS
A	2 remote powered WD + single path signalling
B	1 self powered WD + single path signalling
C	Dual path signalling (no WD)
D	Single path signalling (no WD)

Examples of what some of the Notification Options mean

Grade 2X means that one self-powered audible warning device (WD) is provided as a minimum.

Grade 3B means that one self-powered audible WD and an Alarm Transmission System (ATS) meeting the "ATS 4" performance criteria are provided as a minimum.

Grade 4C means that a main ATS meeting "ATS 5" performance criteria and an additional ATS meeting "ATS 4" performance criteria are provided as a minimum.

Note: *The system can of course be provided with more WDs and/or ATSs than are required to satisfy the minimum requirements.*

The ATS performance criteria are described as "ATS 1" up to "ATS 6" with "ATS 6" having the highest (best) performance. For example Grade 2B signalling must enable the ARC to be notified of signalling failure with 25 hours ("ATS 2"), Grade 3B within 5 hours ("ATS 4") and Grade 4B within 3 minutes ("ATS 5").

Most Insurers will require dual signalling and the ultimate measure of ATS performance is the reporting time following failure of both paths and this is shown below.

ATS path failure condition	Reporting Times						
	ATS6	ATS5	ATS4$_{Plus}$	ATS4	ATS3	ATS2	ATS1
No ATS path failure condition (i.e. Both primary and secondary path(s) operational)	No fault reported	No fault reported	No fault reported	No fault reported	No fault reported	No fault reported	No fault reported

Loss of Primary path* only (i.e. secondary path remaining operational)	20s	180s	10min	300min	25hr	25hr	25hr
Loss of Secondary path only (i.e. primary path remaining operational)	---	300min	25hr	25hr	25hr	25hr	---
Loss of Secondary path whilst operating in 'stepped up' reporting mode (i.e. the loss of Secondary path some time after a previous loss of the Primary path).	---	180s	10min	300min	25hr	25hr	---

Table Note

Where such checking has not already been initiated (for example, upon earlier detection of the possible loss of the primary path), then upon the reported loss of the Primary path immediate checking shall begin to confirm the availability of a Secondary path in order that the loss of all transmission paths within a very short time (for example, caused by the catastrophic failure of the SPT), can be promptly reported to the ARC, i.e. before a secondary path has entered its expected 'stepped up' reporting mode. This checking of Secondary path availability, and where appropriate fault reporting, shall be completed within the maximum failure reporting times shown in Table 6.

Because of the variations available in each Grade of system it is likely that installers and specifiers will continue to identify the method of signalling by proprietary name (see table below) and state the number and types of sounders to be installed (e.g. '2 self-actuating sirens').

Common Signaling Methods	Description
Audible / Bells Only	The system sounds a local bell or siren to attract the attention of neighbors / passers-by.
Auto-dialer	This will automatically, on activation of the alarm, ring pre-programmed numbers in sequence to inform designated individuals / keyholders of the activation. ***Under no circumstances should the police telephone number be programmed into the auto-dialer.***
Digital Communicator	Digital Communicators offer a cost effective means of transmitting signals to an Alarm Receiving Centre (ARC). They connect to a standard telephone line (PSTN) and in the event of an alarm "phone up" the ARC and exchange code information. If the telephone line is cut the ARC is NOT notified and the system reverts to local indication only.
BT Redcare	Redcare is a constantly monitored (polled device) system signaling over the PSTN to the remote ARC. If the telephone line develops a fault or is deliberately tampered with (e.g. by an intruder), the ARC are notified.
Dualcom*	DualCom has two lines of signaling (GPRS and PSTN), known as dual path signaling. If either line is cut or jammed then the other line keeps signaling. If both lines are cut/jammed then this is classed as a confirmed alarm which meets with DD243 requirements.
Redcare GSM*	RedCARE GSM has two lines of signaling (monitored PSTN line and GSM [Global System for Mobile Communications] radio link). If either line is cut or jammed the other keeps signaling. If both lines are cut/jammed then this is classed as a confirmed alarm which meets with DD243 requirements.

***Note:** **Dual path signalling will almost always be required on a commercial installation** because it is capable of transmitting a 'confirmed activation' at all times to the ARC, thus qualifying for police response under the requirements of BS8243. Whereas Intruder & Hold-up Alarm Systems (IHAS) which only incorporate single path signalling will be unable to generate a 'confirmed activation' if the signalling path is interfered with or disabled in any way.*

However, any claim that the scheme described in PD 6662: 2010 has been followed should state that the intruder and hold-up alarm system conforms to PD 6662 for a Grade 1, 2, 2X, 3 or 4 system, with notification (formally signalling) option A, B, C, D or X.

Important: There are now a myriad of companies supplying signalling systems beyond those mentioned above; Webway, Chiron, Emizon, Bold, to name but a few, and each of these may provide a range of different products each with their own claims as to system performance. Where such systems are proposed it is recommended that you refer to your Risk Engineering department for further guidance. In addition many businesses are choosing to transmit signals via IP (internet protocol) and there are additional considerations to be taken into account when considering the suitability of this method. The Loss Prevention Certification Board (LPCB) now has a scheme for testing of Alarm Transmission Systems. ATS products that achieve LPS1277 have been assessed as meeting the relevant parts of BS50131/6: alarm systems plus some additional requirements. Whilst not all products on the market have achieved this certification, the Insurance industry actively promotes its adoption.

Police Response to Security Systems

It is important to note that EN 50131-1 and PD 6662 do not cover the disciplines necessary to design and install a system that provides confirmed activations to which the police will respond.

Therefore in addition to the European Standards you will still need to apply the requirements described in the British Standards Institute document BS8243:2010: "Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions" to installations that signal to an ARC and require a police response as well as the principles contained within the current NPCC (National Police Chiefs' Council) Police Response to Security Systems Policy.

BS8243 states Intruder & Hold-up Alarm Systems (IHASs) should be designed, installed and configured to provide effective confirmation technology to minimise the likelihood of false alarms. Alarm confirmation aims to provide the ARC with high confidence that an alarm signal has been caused by genuine intrusion.

There are three forms of alarm confirmation technology for use with IHASs:-

Audio confirmation technology – when audio is be transmitted from the supervised premises to the ARC for interpretation.

Visual confirmation technology – when images are transmitted from the supervised premises to the ARC for interpretation.

Sequential confirmation technology – when two separate alarm conditions are reported, each originating from an independent detector within the confirmation time (not less than 30 min and not more than 60 min).

NPCC Police Response to Security Systems Policy

The current NPCC policy places security systems into the following two types:-

Type A Security Systems = Remote Signalling Systems terminating at a recognised Alarm Receiving Centre (ARC), Remote Video Response Centre (RVRC) for CCTV and System Operating Centre (SOC) for vehicle tracking. All centres must conform to BS 5979 (Cat II).

Type B Security Systems = All Other Security Systems (e.g. Audible and hybrid alarms, including bells-only and automatic dialling alarms, as well as alarms from non-compliant companies and non-compliant ARCs).

To obtain police attendance, Type B systems will require some additional indication from a person at the scene that a criminal offence is in progress which indicates that police response is required. This will require human intervention such as member of public, owner or agent visiting or viewing the premises. The addition of electronic means to provide confirmation will not promote such systems to Type A or achieve police response.

A Unique Reference Number (URN) will not be issued for Type B systems and there is no guarantee of police response. Type B calls should be passed to the police by public telephone lines or 999 as appropriate. The level of police response will depend on the quality of the information received.

For further information refer the 2018 NPCC ***Summary of Amendments to previous document Guidelines on Police Requirements & Response to Security Systems 2015 version***

https://www.npcc.police.uk/documents/crime/2018/Security%20Systems%20Policy%202018.pdf

Police Attendance – Intruder Alarm Systems

For Type A security systems there are two levels of police response:-

- LEVEL 1 – Immediate/Urgent
- LEVEL 3 – Withdrawn – No police response. Keyholder response only.

All new systems will qualify for a URN (Unique Reference Number) and police response if installed to the scheme described by PD 6662.

Systems issued with a URN will receive LEVEL 1 response until three false alarms have been received in a rolling 12 month period.

Following two false calls in 12 months the customer will be advised in writing, with a copy forwarded to the maintaining company, informing them of the situation and recommending urgent remedial action.

Following three false calls in 12 months LEVEL 3 will apply and police response will be withdrawn. The customer will be advised in writing, with a copy to the maintaining company, who will be required to instruct the Alarm Receiving Centre (ARC) not to pass alarm signals to the police.

Following withdrawal of police response, the following conditions will apply in order to apply to have LEVEL 1 response reinstated:-

I. Confirmed systems will require the cause of the false alarms identified, remedial action taken and a period of 3 months free of false alarms calls (supported by evidence from the security company).

II. Unconfirmed systems will need to be upgraded to a confirmed system in accordance with BS8243:2010 (supported by a copy of the NSI/SSAIB Conformity certificate).

Should the level of false calls result in the restoration of response being delayed for more than 6 months, the URN will be deleted and the customer/security company be advised in writing. It is likely that the Insurer will ask for additional measures to be put in place (e.g. professional keyholding) whilst police response has been suspended.

Police Attendance - Personal Attack (PA) Alarms

Installation and reinstatement of PAs must comply with the BSIA / NPCC Ten Point Plan.

Police response will be withdrawn to the PA part of the IAS after a maximum of 2 false calls in a rolling 12 month period.

Where a system loses response to a PA, the security company should liaise with the end user to see if the PA element is necessary. If it is not required it should be removed.

Police response may be restored following receipt of evidence from the security company that the PA has been free of false calls for a period of 3 consecutive months.

Response may be reinstated to PAs before the 3 month period in the following circumstances:

I. The security company must satisfy the police force concerned that a significant change has been made to that particular system to prevent further false calls. Reinstatement in this way can be obtained only once.

II. An additional form of confirmation has been installed to the system

Keyholders

All premises with Type A systems shall have at least two keyholders, details of whom will be maintained by the ARC/RVRC or through arrangements with a central keyholding service. Keyholders shall be trained to operate the alarm, be telephone subscribers, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified.

Customers who employ a commercial keyholding company must be aware of the Security Industry Authority Licensing Regulations in relation to keyholding and response.

Failure of keyholders to attend when requested on three occasions in a rolling twelve month period, will result in the withdrawal of police response for a three month period. The procedure for reinstatement will be as 3.1.7.

Inspectorates / Governing Body

For security systems to qualify for a URN and therefore be eligible to receive an automatic police response to alarm activations (i.e. Type A) they must be designed, installed and maintained to the required European/British Standards, compliant with the NPCC (National Police Chiefs' Council) Police Response to Security Systems Policy by security companies 'Approved' by one of the following Independent Inspectorates who are registered with the Police:-

NSI (National Security Inspectorate)

Sentinel House, 5 Reform Road, Maidenhead, Berkshire SL6 8BY Tel: 0870 205 0000 Fax: 01628 773367

E-mail: nsi@nsi.org.uk Website: www.nsi.org.uk

SSAIB (Security Systems & Alarm Inspection Board)

Suite 3, 131 Bedford Street, North Shields, Tyne & Wear NE29 6LA. Tel: 0191 296 3242 Fax: 0191 296 2667

E-mail: ssaib@ssaib.co.uk Website: www.ssaib.org

Independent Inspectorates are not-for-profit approval bodies who carry out inspection services for the security industry and protect customer interests. They themselves are governed by UKAS (United Kingdom Accreditation Service), the sole accreditation service recognised by the Government.

Questions to ask when considering the suitability of an intruder alarm installation:

a) Are the installing / maintaining company approved by an independent inspectorate?

b) To what standard has the intruder alarm been installed (will generally be European Standard EN 50131 / PD 6662)?

c) What grade of system has been installed (N.B. Grade 3 generally regarded as a minimum for commercial risks)?

d) What grade of ATS (Alarm Transmission System) has been installed (N.B. Insurers will generally look for a minimum of ATS4PLUS)?

e) Was a risk assessment completed prior to the system being specified (and is a copy available)?

f) Does the system have a URN and is full (level 1) police response in place?

There is further detailed guidance on signalling systems and management of intruder alarms available from the RISC Authority

https://www.riscauthority.co.uk/riscauthority_home/

Disclaimer:

Please note that the Information contained herein has been provided to you for general information purposes only and is considered confidential and/or privileged information, which you must not distribute to any third party, in whole or part, without Protector's express written permission. Whilst all reasonable care has been taken to ensure that the information in this document is comprehensive and accurate, Protector makes no representation, warranty or undertaking, express or implied, as to the accuracy, reliability, completeness or reasonableness of the Information. Any assumptions, opinions and estimates expressed in this document constitute Protector's judgment as of the date thereof and are subject to change without notice. Any projections and/or proposed risk mitigating solutions contained in this document are based on a number of assumptions as to existing risk conditions and there can be no guarantee that any projected outcomes will be achieved, nor that no other risks exist. Protector does not accept any liability for any direct, consequential or other loss arising from reliance on the contents of this document, and provides no guarantee that recommended remediation measures supersede, or replaces any statutory obligations.