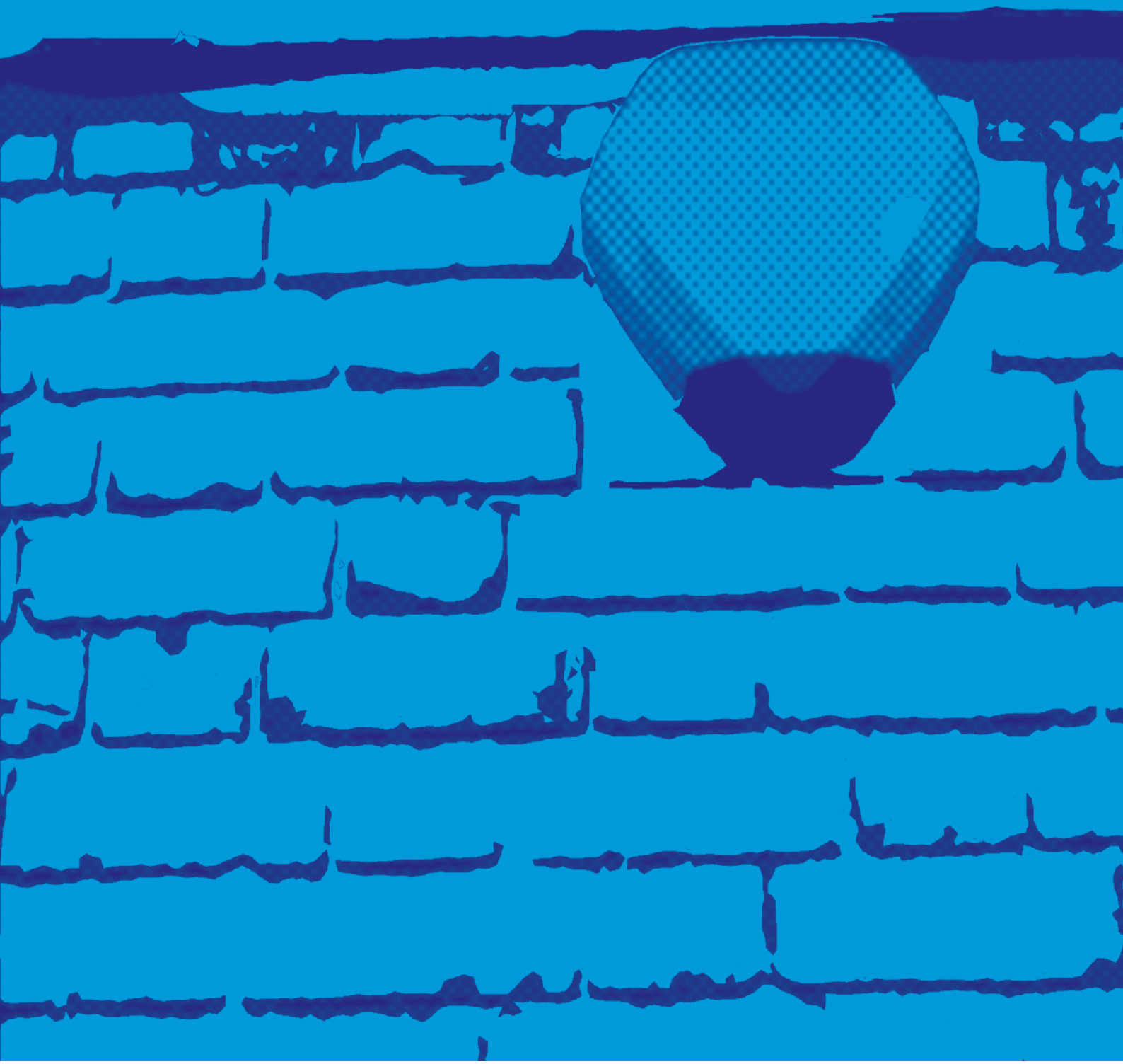
S9
First published 2009
Version 02

Security

Intrusion and hold-up alarm systems (I&HAS): considerations for installers and other stakeholders



RISC Authority
formerly InFiReS

administered by
FPA
Fire Protection Association

Acknowledgements

The assistance of the following with the supply of images for this guidance document is gratefully acknowledged:

Cooper Security Ltd

Pyronix Ltd

IMPORTANT NOTICE

CONTENTS

1. INTRODUCTION

Intrusion and hold-up alarm systems (I&HAS) are an established part of the protective security measures commonly deployed at most commercial, and many domestic, premises against the possibility of theft, robbery, malicious damage and arson. For simplicity the term I&HAS is used throughout this document, although it is possible for an intruder alarm system (IAS) or hold-up alarm system (HAS) to exist independently of each other, as well as in combination.

Those with formal responsibility for the design/specification and installation of I&HAS (referred to hereafter as installers), clearly have an interest in providing good quality and reliable systems. Insurers have a similar interest, whether through requiring new or upgraded I&HAS, or being asked to accept existing systems, since adequate alarm protection is often a requirement for providing certain types of insurance cover.

In the relatively recent past, judging the adequacy of I&HAS for insurance purposes was a fairly simple matter, often summed up in the simplistic phrase, which almost became a mantra, 'NACOSS Redcare alarm'. However, new alarm inspectorates and inspection schemes, developments in detection and signalling technology, the advent of police requirements for confirmed alarm activations and the need for installers to complete a formal security risk assessment, have all contributed to greatly increased complexity when it comes to designing and installing I&HAS. As a result, the old industry mantra is no longer appropriate; installers and insurers needing to account for the now many possible options, requirements and technical complexities of modern I&HAS, especially those intended to elicit a police response.

Alarm purchasers/users (referred to hereafter as customers) will, if asked, usually say that they too want good quality and reliable systems but, often unwittingly, may hinder this outcome by emphasising their desire to minimise financial outlay. In such situations, and with insurers often wishing to see the best alarm protection possible, it can be difficult for installers to offer a system that satisfies both parties. This is especially true if the customer does not think that their insurer needs consulting, or will not otherwise facilitate contact between their insurer and installers.

The increased complexity of new I&HAS aggravates the risk of a significant mismatch occurring between the design of I&HAS, as might be agreed between an installer and a (possibly reluctant) customer, and that which an interested insurer might have wished to see, or encourage, had they been consulted beforehand. Such a mismatch is frequently expensive to rectify retrospectively.

1.1 Scope

When the mismatches between insurers' general expectations and many installed I&HAS are debated in industry forums – particularly in the light of the complex changes in design standards and police response arrangements that have occurred in recent years – insurers are sometimes criticised for not providing the alarm installation industry with clear guidance, both on what they would usually expect to see included in I&HAS, and why. The comment is also often made that in some areas, staff at insurers and insurance brokers would benefit from greater awareness of current I&HAS issues.

These guidelines have therefore been prepared with several intentions, the primary objective being:

- to allow installers better to anticipate, and therefore account for or otherwise inform customers of, any likely current or future insurers' general requirements for new I&HAS, and, by extension, certain modifications to existing systems.

As a secondary aim, they should also:

- help refine insurer/insurance broker awareness of current I&HAS issues and thus enable them better to respond to customers' and installers' queries;
- provide useful information to alarm receiving centre (ARC) operators and intruder alarm equipment manufacturers and suppliers; and
- provide guidance to customers requiring in-depth I&HAS information.

Note: The RISCAuthority is preparing a separate, brief customer guide to new I&HAS.

Whilst much of this guide is written with commercial premises in mind, many of its recommendations will be relevant to domestic premises.

The guidelines do not take account of the security implications of failure of users properly to use I&HAS. For example, failure to set or unset systems correctly, to adequately secure alarm codes/operating devices or heed warnings about system status at the point of alarm setting. Suffice to say that training on such matters is expected as a normal part of an installer's duties for all new or modified systems.

Note: Although installers and insurers have a role to play in providing good advice, the ultimate responsibility for selecting appropriate I&HAS, as with any other security measure, must rest with the customer.

1.2 Structure and use

Because the concept is now familiar to the alarm industry, this guidance document deals with the various topics raised in the context of installers undertaking the widest possible formal security risk assessment. That is, a process by which the equipment used, system design and expected alarm response take account of the likely security risks, coupled with the needs and expectations of customers and any other interested parties, for example, insurers or the police.

Insurers consider risk assessment a potentially helpful process, not only for determining the grade of new I&HAS, as now required by European Standards, but also for the wider design of all systems, including significant extensions or alterations to existing systems and, in particular, the upgrading of existing non-confirmation systems to provide confirmation (in order to reinstate lost police response).

The process of risk assessment is essentially based on asking appropriate questions and making suitable observations on site, then drawing together the information obtained to design an I&HAS that avoids or minimises the risks identified.

In many situations there will be no standard solution resulting from a risk assessment. Installers and those they seek advice from – insurers, for example – will therefore need to make a judgment based on their own experience and understanding of the risks faced. However, a risk assessment that does not at least consider all the issues outlined in this guidance document will arguably be at risk of being incomplete.

This guidance document includes a bulleted summary of insurers' typical I&HAS requirements (see section 2 of the guidance document). The rest of the document then expands on the points listed; starting with clarification of insurers' likely thought processes behind the decision of which grade of I&HAS is likely to be most appropriate. It then moves on to provide advice on other equally important risk-related matters regarding system design, hold-up facilities, signalling, alarm response, security fog devices and related alarm documentation.

The guidance given assumes that premises are of typical construction and have an appropriate (usual) level of physical security and occupancy commensurate with the nature of their use and the area in which they are located. Where this does not apply, the design features of I&HAS may need to be modified to reflect this.

In addition to these general guidelines, a specific approach to any interested insurer for comment and approval of proposals for a new system, or alterations to an existing system, is always recommended – particularly for higher risk or more complex cases.

1.3 Insurer liaison

Not all premises or risks will be insured but where insurers are involved they may expect or require their customers to have I&HAS of a particular type – typically a remotely monitored alarm system with police response via a URN.

In such cases, insurers may already have provided an outline or detailed alarm specification adequate to guide installers, or have otherwise provided a contact for further discussions. In other cases, the insurer may be unaware of their customer's proposals for a new or altered I&HAS, but it is clearly desirable that they be consulted before any work proceeds.

A key advantage of obtaining insurer guidance is that installers are then quoting against others on a level playing field – that is, not competing in terms of the grade or basic functions of proposed I&HAS. Installers encouraging and obtaining insurer input may also find insurer support helpful in obtaining the customer's agreement to other specific I&HAS design proposals, especially in the face of competition from other installers proposing a lower level of protection. In short, insurer involvement can be a potential selling aid.

Note: An insurance policy may contain a policy condition that requires the policyholder to obtain the insurer's agreement to any changes to existing I&HAS. Failure to comply with this may jeopardise insurance cover. Installers may therefore consider it prudent to alert customers to this possibility when recommending insurer comment on I&HAS.

It has to be acknowledged that, for various reasons, establishing contact between installers and any interested insurer can prove problematic. For example:

- the customer may not wish to disclose details of their insurer;

  or

- the customer may not know who their insurer is, or may not be readily able to identify them, for example, the ultimate insurer may stand behind a broker or marketing organisation.

Whilst it is therefore generally preferable for the customer to contact their insurer and then provide suitable information to installers, there will be occasions when customers ask installers to initiate the process. In such cases, a customer is often more readily able to identify who arranges their insurance cover – that is, their insurance intermediary (such as an insurance broker) – than to identify the actual insurer. So initial contact with the intermediary is recommended in most cases.

In doing so, installers should bear in mind that:

- the intermediary may not feel able to discuss insurance- or security-related matters unless the customer has provided verbal or written authority;

  and

- the intermediary may know relatively little about I&HAS or insurers' likely alarm requirements;

  or

- rather than risk inadvertently giving inappropriate advice, they may suggest contact is made direct with the insurer, who they will be able to identify. In such circumstances, it is worth a little further effort or delay in making appropriate contact with the actual insurer.

Once the insurer is identified, contact can be made. But, in doing so, installers should bear in mind that:

- the insurer may not feel able to discuss insurance or security related matters until the intermediary or customer has provided verbal or written authority;

  and

- making contact with the insurer's office/telephone call centre responsible for the case may involve several onward referrals;

  and

- senior underwriters or members of the insurer's risk survey team will usually be best placed fully to discuss and advise upon requirements for I&HAS;

  or

- ultimately, particularly on small cases, insurers may not wish to impose requirements or otherwise offer advice on proposed I&HAS.

In many cases, it may therefore prove easier for installers to ask the intermediary to provide a pre-alerted named contact at the insurer with whom installers can then more readily discuss the matters at hand.

2. SUMMARY OF TYPICAL INSURER REQUIREMENTS

Insurers' main requirements for new I&HAS are listed in Table 1. The remainder of this guidance document provides a full explanation, plus insurers' views on other I&HAS issues.

Table 1: Insurers' main requirements for new I&HAS

- **Installation/maintenance**

  An installer holding National Security Inspectorate (NSI) or the Security Systems Alarm Inspection Board (SSAIB) approval.

  An installer eligible to apply for a police unique reference number (URN) with the police force in whose area the alarmed premises are located.

  Contract in force for routine and emergency maintenance.

- **Equipment**

  Grade 3 for most commercial risks, Grade 2 for most domestic risks.

  Control and signalling equipment installed out of sight, and NOT located in an area used as an alarm entry-exit route.

  Customers unable to omit detectors unless part of pre-agreed part set.

- **Non-confirmation systems**

  Appropriate detection in each at-risk area.

  Single path signalling (see * below).

- **Confirmation systems (DD 243/BS 8243)**

  Sequential confirmation used.

  Two appropriate forms of detection in each at-risk area.

  Means of unsetting to be via clause 6.4.3, unless entry route or premises are considered low risk, in which case use clause 6.4.5.

  Dual path signalling (see * below).

- **Hold-up alarm systems (where required)**

  Dual path signalling (see * below).

- **Signalling**

  * A remotely monitored product with fault reporting times at (or near) Grade 4 requirements.

  Dual path systems to have stepped up fault reporting on the secondary path once the primary path has been lost.

- **Alarm Receiving Centre (ARC)**

  A continuously manned centre with NSI or SSAIB approval.

  Police (where eligible) and keyholders notified of alarm events/faults as soon as they are notified to the ARC operator.

- **Response**

  Police, in accordance with the responding force's version of the Association of Chief Police Officers' (ACPO, ACPOS in Scotland) Security System Policy (SSP).

  Appointed keyholders, owners/staff/friends or a response company.

  Note: Where a response company is used, one that holds NSI or SSAIB approval and does not store premises keys and/or alarm operating codes or devices at the customer's premises – in a key box, for example.

- **Security fog devices (where required)**

  Compliance with BS 7939 (or BSEN 50131-8 when implemented in UK).

  Loss of mains power monitored and promptly notified to the ARC.

- **Documentation**

  Copy of the specification – that is, (as appropriate) the system design proposal and/or the as fitted document (SDP/AFD), including details of ARC responses to alarm and other signals.

  Copy plan showing premises layout and the scheme of detection.

3. INSTALLATION/MAINTENANCE

Insurers want to be sure that alarm systems are designed, installed and maintained by suitably trained, competent and trustworthy personnel in accordance with relevant British/European Standards*. Because of this, and associated police requirements for the issue of URNs, they usually expect installers of I&HAS to hold the relevant approval of a police recognised, UKAS accredited inspectorate, namely, NSI or SSAIB. In some cases, insurers may also wish to see evidence that installers comply with a formal quality management system – ISO 9001, for example.

* Currently, standards in the BS EN 50131/50136: **Alarm systems. Intrusion and hold-up systems** series, as implemented in the UK by PD 6662 (the 'Euro Standards'). It is expected that the provisions additional to BS EN 50131-1: **Alarm systems. Intrusion and hold-up systems. System requirements** for maintenance, currently embodied in PD 6662: **Scheme for the application of European Standards for intruder and hold-up alarm systems**, will be replaced by DD 263: **Intruder and hold-up alarm systems. Commissioning, maintenance and remote support. Code of practice**, publication of which is expected late in 2009. In addition, where police response is required, DD 243: 2004: **Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice** (to be replaced by the current draft BS 8243: **Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice**, expected to be published in 2009) will be applicable.

4. EUROPEAN STANDARDS

The European Standards for I&HAS (Euro Standards) apply to all new I&HAS and describe four grades of system and alarm signalling, based on progressively increasing alarm protection (referred to as supervision in the Euro Standards) to match increasing security risk. Reference is also made to considering the risk of, and the desired degree of resilience against, possible attack or interference with I&HAS by a notional intruder with defined levels of I&HAS knowledge, and the likely availability of certain tools and equipment that might assist them.

Installers are also expected to select and use equipment that meets a suitable Environmental Class, ranging from I to IV, reflecting exposure to potentially detrimental temperature and humidity or weather conditions.

Selecting an appropriate grade assumes particular significance in the light of the fact that a system of one grade cannot later be changed to another without possibly having to change some, if not all, of the installed components. In some circumstances, it may be necessary, in effect, to install a completely new system.

The various grades of I&HAS can briefly be summarised as:

- *Grade 1 – low risk*

  Intruders are expected to have: little I&HAS knowledge and a limited range of easily available tools.

  Key system features are: no tamper alarm for detection devices/junction boxes, no event recording (alarm log) and a 12-hour battery back up.

  Alarm signalling options include: a site warning device (WD) only or a remotely monitored single path system.

- *Grade 2 – low to medium risk*

  Intruders are expected to have: limited I&HAS knowledge and a general range of tools and portable instruments.

  Key system features are: tamper detection for all components, 250-event log, and 12-hour battery back up.

  Alarm signalling options include: a site WD only (Grade 2X), a remotely monitored single path system (with or without a WD), or a remotely monitored dual path system (no WD).

- *Grade 3 – medium to high risk*

  Intruders are expected to be: conversant with I&HAS and have a comprehensive range of tools and portable instruments.

  Key system features are: as Grade 2 plus the ability to detect masking (covering) of movement detectors or to detect or prevent their re-orientation (being moved), a 500-event log and a 24-hour battery back up – reduced to 12 hours if loss of mains power is signalled to an ARC.

  Alarm signalling options include: a remotely monitored single path system (with or without a WD) or a remotely monitored dual path system (no WD).

- *Grade 4 – high risk*

  Intruders are expected to have: the ability or resource to plan an intrusion/robbery in detail and a full range of equipment, including means for substituting I&HAS components.

  Key system features are: as Grade 3 plus the ability to detect reduction in range of movement detectors and a 1,000-event log.

  Alarm signalling options include: a remotely monitored single path system (with or without a WD) or a remotely monitored dual path system (no WD).

Note: Although certain signalling options are described at each grade, it is permissible to exceed these, for example, a WD (of suitable grade) can be added to I&HAS with dual path signalling, or Grade 4 signalling used with I&HAS that otherwise meet a lower grade, for example, Grade 2 or 3. Indeed, such enhancement is often expected by insurers in the UK, as indicated elsewhere in this document.

4.1 Insurers and grading

With the introduction of the Euro Standards, many installers asked the insurance industry to indicate how they would align the four 'Euro grades' with the various risk types which they might typically encounter.

By way of general guidance, the IPCRes working group (forerunner of the RISCAuthority Security working group) published a document titled **Intruder alarms and a harmonised European Standard**. This is available to view, or as a free download, via *www.riscauthority.co.uk*. This document outlined the background to the introduction of the Euro Standards, the main features of each grade and insurers' likely use/acceptance of each grade based on their respective benefits.

With regard to grading, IPCRes advised insurers to consider detection/control equipment and alarm signalling as separate aspects of I&HAS and summarised insurers' likely position as follows:

Detection and control equipment

- Grade 1 – inadequate for insurers' needs.
- Grade 2 – suitable for most domestic and some low risk commercial premises.
- Grade 3 – suitable for most commercial and some high risk domestic premises.

Note: This is the safe default position for installers uncertain of insurance requirements.

- Grade 4 – suitable for very high risk premises.

Signalling

- Unless only localised (audible only) signalling is required (Grade 2X), remote signalling was likely, for the time being, to be specified by products of known performance rather than generic grade.

Note: The system of grading set out in the Euro Standards implies that a system using, for example, Grade 2 detection and control equipment would also, by default, use Grade 2 signalling. However, because of certain requirements for signalling systems used within the UK and ambiguity over some of the signalling requirements in the Euro Standards, where remote signalling is required, insurers will usually want signalling that performs at (or near) Grade 4 requirements, irrespective of the grade of the I&HAS detection and control equipment.

See section 8.2 for further information on insurers' typical remote signalling requirements.

4.2 Risk assessment – determining grade

Installers are required to undertake and record a formal security risk assessment to help determine the grade and design of I&HAS appropriate to customers' premises.

This assessment should take account of the nature of the premises and contents in relation to the risk of theft/burglary or hold-up and, if only because of the grading structure of the Euro Standards, account should also be taken of possible means by which criminals may attempt to interfere with I&HAS prior to, or during, an intrusion.

Extensive formal guidance on matters to consider on the subject of building and contents security, plus technical equipment related issues, is contained in EN 50131-7: **Application guidelines**.

Whilst there is no specific requirement to consider the security of people in EN50131-7, namely staff normally present or likely to attend as keyholders, nor of police response requirements, these are issues of potential significance in the UK, especially in the context of confirmation systems. However, attention to these matters during a risk assessment is implied, insofar as Section 6.7: Consultation of the **Application guidelines** recommends that system design should be 'determined in consultation with any other interested parties, for example, insurers or police'.

As providers of liability insurance, insurers often have, in the context of the design of I&HAS, a commercial as well as moral duty to consider the safety of keyholders. This is because policyholders will often ask employees, or private individuals, to attend premises as keyholders in response to alarm and fault signals. If, because of inadequate I&HAS design, keyholders find themselves attending premises alone and without routine police back up after intruder generated alarm activations or alarm equipment/signalling system faults, they may be at risk of injury from intruders waiting at, or actually present in, the premises. In the event of an attack then being made upon keyholders, the possibility exists of a liability claim being made against an employer (the policyholder) for exposing them to danger that could have reasonably been foreseen and avoided by better design of the I&HAS.

4.3 Risk assessment – installer methodology

4.3.1 Basic risk assessments

The grade-related security risk assessments of some installers can appear (to insurers) to be limited to rather basic factors such as the:

- occupation/trade at the premises;
- nature of the target items (those items usually considered attractive to thieves);
- values at risk;
- at-risk areas (rooms/areas where target items are located within the premises);
- premises location/crime history;
- physical security of the premises – that is, doors, windows, walls and roof; and
- loss history.

These are all valid considerations, but arguably they have a tendency to restrict a risk assessment to considering the likelihood of, or the possible entry point for, a break-in and the values of tangible items that may be stolen.

4.3.2 Wider risk assessments

Insurers will often consider the following additional aspects of risk assessment, and installers are therefore encouraged to build them into their risk assessment processes:

- *Vulnerability of I&HAS to interference* – As the possibility of interference with, or compromise of, I&HAS is one of the risk factors mentioned in the Euro Standards, and one with the potential to create a large loss (for example, if the I&HAS fails to work after such an eventuality), insurers tend to give significant weighting to this aspect of risk when determining their grade requirements, and especially in the context of the need to detect possible interference with remote signalling promptly.

- *Quickly obtaining confirmed activations* – Insurers will give considerable weight to the need to obtain confirmed, rather than unconfirmed, alarm activations as soon as possible during any break-in, in order to elicit the earliest practicable police response.

- *Keyholder safety* – In the context of obtaining an early confirmed activation, and thus early police intervention, insurers may also consider keyholder safety risks. In particular, they are anxious to avoid the risk of keyholders attending unconfirmed activations where, due to inadequate levels of detection, intruders may be in the premises.

- *Business interruption* – In addition, and generally only at commercial premises, insurers will consider the risk of business interruption – that is, the loss of trading potential or business reputation following a break-in and theft of items or records or damage to premises or machinery, for example, computers.

See sections 6, 8.2 and 10 for further information on, respectively, insurers' typical requirements for confirmation system design, remote signalling and response arrangements.

4.4 Risk assessment – insurers' grade considerations

Rather than starting with Grade 2 and looking for reasons why a higher grade may be appropriate, insurers tend to start from the default position that the best possible system should always be proposed, unless there are risk-based, or sometimes commercial, reasons to accept lesser protection.

For the purposes of this guidance document, the process of selecting a suitable grade of I&HAS can be simplified by ignoring signalling for the time being (see section 8). It is also helpful to initially consider the potentially limited application for Grade 1 and Grade 4 detection and control equipment, that is:

- Grade 1: inadequate for insurers' (and many customers') needs; and
- Grade 4: suited to very high risk premises, for example, those that contain items of very high monetary, historic or cultural value and/or which undertake a critical business, financial, military or national function

Therefore, for all practical purposes the choice of I&HAS grade for insurers is likely to be between Grades 2 and 3. When considering this choice, insurers will usually take account of a number of risk-related factors, as indicated below.

4.4.1 When is Grade 3 appropriate?

At many commercial, and a few domestic, premises the nature and value of target items present, coupled with the crime risk, will be such that a Grade 3 system will clearly be appropriate. Where there is doubt as to the values and attraction to criminals of target items or other aspects of the premises risk, consider the potential benefit of a Grade 3 system in line with the following criteria:

• Is there a risk of interference with alarm equipment?

Consideration should be given to the risk that persons may attempt to compromise or disable alarm protection – particularly where persons (employees or the public) may have access to all or key parts of a premises.

Fig 1: Movement sensors can be vulnerable to interference

A feature of most workplaces is that employees are likely to have unsupervised access to alarm equipment, and those with large or transient workforces may be considered to have a greater than usual risk of someone being able and tempted to compromise alarm detection during working hours.

A feature of most shops, pubs, clubs, hotels, schools and leisure facilities is that members of the public may have unsupervised access to alarm equipment (alarm detectors in particular) during the hours when they are open for business.

In all such cases, a particular feature of Grade 3 systems, the use of anti-mask movement sensors, for example, with their additional protection against reorientation, should indicate that Grade 3 I&HAS are likely to be appropriate, unless:

- employees are a small group of trustworthy people, for example, family, friends or those of long-standing, stable employment;

  or

- employees are subject to some form of formal security screening, for example, to BS 7858: **Security screening of individuals employed in a security environment. Code of practice**;

  or

- employees are well supervised and/or do not have general access to all or key at-risk areas;

  or

- there are no employees;

  and

- there is no public access to the premises (for example, most homes), or, if there is public access, vulnerable movement sensors can be located in those areas to which the public would not readily have access, such as behind, or adjacent to, a permanently manned shop counter.

Note: In some cases, even though the factors mentioned above may suggest that a Grade 3 system is appropriate, the potential financial loss (in terms of the value of target items or the loss of trading potential/business reputation, etc) following pre-planned compromise of the I&HAS, may be sufficiently low that the customer is willing to accept a Grade 2 system. However, before proceeding on such a basis it would be especially prudent to check the views of any interested insurer.

• Is there a risk of limited alarm interference?

At some premises, the use of Grade 3 equipment may seem appropriate to protect target items in only one higher risk portion of a generally lower risk premises, for example, use of anti-mask movement sensors in a public access trade counter or showroom attached to a non-public warehouse. Where an area requiring Grade 3 equipment is small compared to the rest of a much larger premises, insurers might accept I&HAS that incorporate a sub-system*, in order to minimise the overall cost; that is, use of Grade 3 control and detection equipment for the higher risk area and (cheaper) Grade 2 equipment elsewhere.

Note: Where this approach is adopted, the official grade of the overall system has to be certified having regard to the lowest graded components used within it – Grade 2 in the example mentioned above.

* Although the term is not recognised in the Euro Standards, these systems are sometimes referred to as hybrid systems.

4.4.2 When is Grade 2 appropriate?

If a Grade 3 system does not appear to be appropriate, consider a Grade 2 system subject to the following proviso:

• ***Is there a risk of future inadequacy?***

One thing insurers routinely consider in relation to I&HAS is the likelihood of changes in the security risk profile. For example, the possibility of a customer embarking upon a change of business direction or increasing possibly modest current values of target items to reflect new trading patterns/fashions, or the deployment of new technology, for example, installing a valuable computer system.

If a Grade 2 system is installed now (notwithstanding that the current insurer may accept it), the risk should be borne in mind that the relatively minor current cost saving (compared to installing a Grade 3 system), may appear to the customer to be a false economy if they are later faced with significant costs of meeting their existing insurer's revised, or a new insurer's future, requirement for a Grade 3 system.

Whenever premises appear borderline for a Grade 2 system, it is particularly recommended that the installer encourages the customer to seek their insurer's advice and, at the same time to offer, alongside a quote for a Grade 2 system, a future-proof quotation for a Grade 3 system.

4.5 Summary of grading issues

Determining a suitable grade of detection and control equipment for I&HAS is only the first step towards designing an alarm system that is appropriate to the risk and the needs of the customer, their insurer or the police.

Whilst insurers may take a pragmatic view on acceptance of systems already installed at Grade 2, when they would have perhaps preferred Grade 3, they will be less sanguine about accepting many other aspects of I&HAS that may not meet their expectations, such as levels of detection/confirmation, methods of unsetting, signalling and response arrangements.

Insurers would therefore encourage installers to highlight, and give equal consideration to, various other risk-related alarm design factors when conducting their risk assessments, as outlined in the remainder of these guidelines.

5. NON-CONFIRMATION SYSTEM DESIGN

Because of current police rules, non-confirmation systems will these days only be installed where I&HAS are proposed with audible-only signalling, or with remote signalling but no requirement for police response via a URN.

As such, system design is a far more straightforward affair than will often be the case with confirmation systems (see section 6) but, nonetheless, installers should still ensure that their risk assessment takes account of certain basic risk and design matters.

5.1 Site equipment

• ***Is there a risk of intruders attacking the control and signalling equipment?***

Control and signalling equipment, more formally termed control and indicating equipment (CIE) and alarm transmission equipment (ATE) respectively, is vital to the ability of I&HAS to process and transmit alarm information. If it can be reached and attacked before a suitable signal has been transmitted, the I&HAS may not fulfil its intended function and, if remote signalling fault reporting depends wholly or partly on local interface monitoring within the ATE, loss of the signalling links to the ARC may either not be detected at all, or not until some time after an attack.

As such, the CIE and ATE (including any modem/router if IP signalling is used), should be located in an area where it is not in public view and is least vulnerable to deliberate attack. It therefore follows that an intruder should also not be able to reach the CIE/ATE (including any modem/router if IP signalling is used), without creating an immediate alarm condition, which would normally preclude it being sited in an area that comprises part of an alarm entry-exit route.

• ***Is there a risk of intruders entering at-risk areas without creating an alarm activation?***

The system should be designed to generate an alarm activation from all at-risk areas within a premises, and as soon as possible after an intruder enters them*.

In this regard, it is also important that the customer is not able to isolate detectors or omit zones of detection except as part of a pre-programmed 'part setting' arrangement agreed with any interested insurer.

* The provision of early perimeter detection, perhaps better to respond to a smash-and-grab style raid, or to cover possible early approach routes to at-risk areas, should not be overlooked.

5.2 Unsetting

Unsetting of non-confirmation I&HAS will usually involve use of an inputted code or fob at an unsetting point inside the premises.

• ***Is there a risk of intruder detection being delayed?***

To allow customers to enter the premises and unset the system, without creating an alarm condition themselves, an agreed alarm entry-exit route and alarm entry time (maximum of 45 seconds), needs to be established. Activation of the first detection device on the entry route, a contact on the entry door, for example, initiates the entry time, during which period any activated detection devices covering the entry-exit route are prevented from generating a full alarm condition. If any non-entry route detectors activate during the entry time, an alarm condition can be generated at the expiry of the entry timer (if the system is an audible-only type) or, for remotely monitored systems, the expiry of a further 30 second period (the abort time). The abort time is intended to allow a customer who has created a false alert extra time to cancel it by unsetting the alarm properly. In such circumstances, this means that a time window of up to 75 seconds (45 plus 30) exists, during which an intruder could make further progress into the alarmed premises without an alarm signal being transmitted to the ARC.

As a result, the potentially delayed alarm response time when using an entry-exit route related means of unsetting should always be borne in mind. This delay may assume even greater significance at higher risk premises given that, in addition, ARCs may be holding (due to police requirements for alarm 'filtering') any alarm activation they receive for up to 120 seconds before presenting it to an ARC operator for action – in order to allow customers time to cancel a possible false alert they have created.

In general, both the entry-exit route and entry time should be limited, respectively, to the minimum area and time practicable, in order to minimise the risk of an intruder (forcing entry via the entry-exit door) going undetected or having their detection unduly delayed.

In a similar vein, if target items are located in, or close to, an area needing to be designated as an alarm entry-exit route where the customer uses a particular door for entry, consideration should be given to suggesting they instead use another, less vulnerable, door (if available) as the entry-exit door.

5.3 Signalling

With remote signalling often being the weakest link in the overall alarm system, a signalling product that enables the ARC to be promptly made aware of loss of the communication path should always be used. While single path signalling may suffice, the benefits of dual path signalling should not be overlooked.

See section 8.2 for further information on insurers' typical remote signalling requirements.

6. CONFIRMATION SYSTEM DESIGN

The police are keen to reduce the number of false alarm activations they are requested to attend. As a result, current police rules for providing a response to I&HAS are often conditional upon providing a confirmed activation – that is, receipt of a second alarm activation signal or piece of related information at the ARC, which suggests that an initial alarm activation signal was not a false alert.

As the sole purpose of a confirmation system is to qualify for and elicit a police response, it is very important to ensure that the risk-assessed design of the I&HAS does in fact enable the desired police response to be reliably obtained, and then early enough during any break-in or robbery to be effective. The overall aim should be to enable the attendance of the police quickly enough to apprehend criminals and to protect staff and keyholders and their property.

The design rules for confirmation I&HAS contained in document DD 243 are complex. Given DD 243's impact on the ability of I&HAS and ARCs to generate a request for police response, various design risks need to be carefully considered.

6.1 Confirmation technology

There are three recognised ways of obtaining confirmed alarm activations, which can be briefly summarised as:

- audio* confirmation – premises microphones transmit sound to the ARC;
- visual* confirmation – premises cameras transmit images to the ARC; and
- sequential confirmation – two or more alarm events are noted by the ARC within a pre-set 30- to 60-minute period (the confirmation time).

* Audio and visual confirmation systems must also have a back-up sequential capability.

Of these three forms of confirmation technology, sequential confirmation is now almost exclusively used. However, that is not to say that it will always be the most appropriate technology.

• Is there a risk of using an inappropriate confirmation technology?

For example, if a building with fragile or lightweight walls is being used as a warehouse and has target items stored against the perimeter walls it can be difficult to install sufficient detectors of two differing technologies, as required by DD 243, in order to obtain a sequentially confirmed alarm activation should an intruder break through the wall and remove items from outside.

In such circumstances, it may be more appropriate, and easier, to install one form of perimeter detection and use audio confirmation to allow an ARC operator to listen in after an activation of a perimeter detector, with a view to determining an appropriate response.

6.2 Site equipment

• Is there a risk of intruders attacking the control and signalling equipment?

Control and signalling equipment (CIE/ATE) is vital to the ability of I&HAS to process and transmit alarm information. If it can be reached and attacked before a suitable signal has been transmitted, I&HAS may not fulfil their intended function and, if remote signalling fault reporting depends wholly or partly on local interface monitoring within the alarm transmission equipment (ATE), loss of the signalling links to the ARC may either not be detected at all, or not until some time after an attack.

As such, CIE/ATE (including any modem/router if IP signalling is used), should be located in an area where it is not in public view and is least vulnerable to deliberate attack. It therefore follows that an intruder should also not be able to reach the CIE/ATE (including any modem/router if IP signalling is used), without creating a confirmed alarm. This would normally preclude it being sited in an area that comprises part of an alarm entry-exit route.

Fig 2: The main control panel should be installed out of sight and in a secure area

• Is there a risk of intruders entering at-risk areas without creating a confirmed activation?

Because the activation of a single detector cannot result in the ARC calling the police, the system should be designed to generate a confirmed activation from all at-risk areas as soon as possible after an intruder enters them. (The provision of early perimeter detection, perhaps to better respond to a smash-and-grab style raid, or to cover possible early approach routes to at-risk areas, should not be overlooked.)

In this regard, it is particularly important that the customer is not able to isolate detectors. It is also important that the customer is not able to omit zones of detection except as part of a pre-programmed part setting arrangement agreed with any interested insurer.

6.3 Means of unsetting

DD 243 contains five methods by which an alarm can be unset, each aiming to reduce the potential for user-generated false alerts when unsetting the alarm system.

They are referred to by their DD 243 clause numbers and titles, as follows:

- 6.4.2 preventing entry until the alarm is unset;
- 6.4.3 preventing entry until confirmation is disabled;
- 6.4.4 opening the entry door disables confirmation;
- 6.4.5 completion of unsetting using a PACE (portable ancillary control equipment); and
- 6.4.6 unsetting carried out in conjunction with the alarm receiving centre.

• Is there a risk of intruders entering the premises without creating a confirmed activation?

Whilst all the aforementioned means of unsetting are permitted in DD 243, their general desirability depends on the degree to which they permit or prevent I&HAS from differentiating between forced or legitimate opening of an alarm entry-exit door. At their worst, in the event that an intruder forces entry via a designated alarm entry-exit door, some of the means of unsetting can effectively prevent the police from being called at all or until it is too late for the response to be effective.

Note: Although various forms of unsetting are permitted by DD 243, the very clear weakness of one clause, 6.4.4, is recognised insofar as installers are required to include a warning about the effects of using it in their system design proposals.

The security risks associated with each are outlined in the following summaries of the operation and effects of each clause. In considering them, installers should take note of insurers' likely stance on each method and have regard to the assessed risk of a break-in via the designated alarm entry-exit door (by, for example, considering its location, build strength and lock security), the length of any programmed entry time and the abort time, coupled with the proximity of the entry-exit door and entry route to any target items.

DD 243 Clause 6.4.2

This clause requires a lock on the entry door to be linked to the I&HAS. Full unsetting of the alarm occurs by the simple act of unlocking the lock or, from the outside of the premises, turning off the alarm using a suitable alarm operating device or code, which in turn releases the lock.

The main benefit is:

- forcing open the entry door can start the process of generating a confirmed activation.

The main weakness is:

- lost or stolen premises keys or alarm operating devices can jeopardise security until the loss is noted and reported by customers and a new lock or operating device is fitted.

Means of unsetting 6.4.2 may be accepted by insurers at premises with expected good key or alarm operating device control; small family businesses, for example.

DD 243 Clause 6.4.3

This clause requires a lock on the entry door to be linked to I&HAS, as in 6.4.2. Partial unsetting of the system occurs by unlocking the door, which then turns off the system's confirmation capabilities or, from the outside of the premises, turning off confirmation by using a suitable alarm operating device or code. In both cases, with the lock opened, customers can enter and complete unsetting inside.

The main benefits are:

- forcing open the entry door can start the process of generating a confirmed activation;
- lost or stolen premises keys or alarm operating devices do not allow complete unsetting of the system; and
- where appropriate, a duress facility can be included.

Note: In such cases, police response will require I&HAS to meet Grade 4 (or, if a pre-Euro Standards system, BS 7042: **Specification for high security intruder alarm systems in buildings**).

Means of unsetting 6.4.3 will usually be insurer's default preference unless:

- there are no, or very few, target items located in, or immediately adjacent to, the designated alarm entry-exit route;

  or

- the alarm entry-exit door is unable to be readily fitted with a suitable alarm-linked lock whether mechanical or electronic (such as a magnetic lock). This may arise, for example, if the door is made entirely of glass and an alternative entry door cannot be utilised. In such circumstances, insurers would normally consider unsetting as per clause 6.4.5 – see below.

DD 243 Clause 6.4.4

This clause requires that opening of the designated alarm entry-exit door trips an entry/exit route alarm sensor which turns off the system's confirmation capabilities, the customer undertaking unsetting inside.

The main weakness is:

- forcing open the entry door disables confirmation throughout the premises.

Means of unsetting 6.4.4 will not normally be accepted by insurers unless:

- *the premises are unusually low risk and/or the entry door is particularly secure (and therefore very unlikely to be forced open) compared to other potentially accessible, and weaker, doors or windows elsewhere in the premises.*

DD 243 Clause 6.4.5

This clause requires that opening of the alarm entry-exit door turns off the system's confirmation capabilities on the designated entry route, with final unsetting then being undertaken inside the premises using a keyholder-carried portable fob or transmitter. If the fob or transmitter fails to work, or the customer has forgotten to bring it with them, unsetting is permitted by inputting a keypad code – but only after the entry time expires.

Fig 3: A typical portable transmitter

The main benefits are:

- lost or stolen alarm fobs and transmitters can, once the loss is noted and reported, be deleted from the system; and
- a shorter than usual entry time can be programmed, customers being able to very rapidly use their fob or transmitter to unset the system.

The main weaknesses are:

- forcing open the entry door disables all confirmation during the alarm entry time (max of 45 secs). However, if any non-entry route detectors activate during the entry time, a further 30-second period (abort time) commences during which no alarm activation can be transmitted from site (to allow a customer who has created a false alert extra time to cancel it by unsetting the alarm properly). In such circumstances, this means that a time window of up to 75 seconds (45 plus 30) exists, during which an intruder can make further progress into the alarmed premises without an alarm signal being transmitted to the ARC. As a result, the potentially delayed alarm response time when using this means of unsetting should always be borne in mind. This delay may assume greater significance at higher risk premises given that, in addition, ARCs are required (because of police requirements for alarm filtering) to hold any unconfirmed alarm activation they receive for up to 120 seconds before presenting it to an ARC operator for action, in order to allow customers time to cancel a possible false alert they have created, for example, via a telephone call to the ARC;
- once the entry time, and any other time delays, expire, audio and visual confirmation systems may be used by ARC operators to try and obtain a confirmed activation in the entry-exit route area, or elsewhere. However, with sequential systems a confirmed activation can only be generated after two* or more detection devices have been activated in parts of the premises not forming the designated entry-exit route; and
- lost or stolen fobs and transmitters can jeopardise security until the loss is noted and reported by customers and the missing device is deleted from the system.

* This will change to one detection device if DD 243 is replaced by the current draft BS 8243: **Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice**.

Note: If fob unsetting is proposed, the potential adverse effect on generating a police response, following a break-in via the entry door, should always be considered as part of the security risk assessment.

A simple example of where use of 6.4.5 might not be appropriate would be a high street shop with an off-street entry door, coupled with an open-plan retail area where most of the target items are on display. If the entry door is a likely forced entry route, and most or all of any movement sensors within the shop are programmed as entry-exit route detectors, use of 6.4.5 will mean that the ability of the system to create a confirmed activation during such a break-in will, depending on the confirmation technology used, be either unacceptably delayed or prevented.

In such cases, if use of 6.4.5 is proposed, it would be unwise for an installer to refer to the I&HAS as a police response alarm without clearly mentioning such a fundamental limitation.

Means of unsetting 6.4.5 will usually be accepted by insurers subject to:

- *the entry door being particularly secure (and therefore unlikely to be forced open) compared to other potentially accessible, and weaker, doors or windows elsewhere in the premises;*

  or

- *there being an internal lobby/entry room, ideally lockable from the remainder of the premises, that can be designated as the alarm entry-exit route;*

  or

- *there being provision made for a virtual lobby – that is, a very small area just inside the entry door, ideally marked by a mat or floor markings, where customers can present their fob or transmitter to an adjacent fob reader before entering further into the premises. Any movement detectors covering the area immediately beyond this virtual lobby must be so located that they do not need to be programmed as entry-exit detectors, for example, being installed adjacent to, but facing away from, the edges of the virtual lobby;*

  and

- *there being no, or very few, target items located in or immediately adjacent to the designated alarm entry-exit route.*

Note: Where target items are located close to an existing entry-exit door, use of 6.4.5 may become more suitable if arrangements can be made for customers to use a different, less vulnerable, door (with an associated lower risk entry-exit route) to enter the premises.

DD 243 Clause 6.4.6

This clause requires unsetting to be undertaken in conjunction with the ARC. It is rarely used as there are no set rules as to how it may securely be done and, as it requires real time communication with the ARC, it is likely to tie up limited resources, particularly at busy times in the ARC.

Means of unsetting 6.4.6 may be accepted by insurers in limited circumstances, and where the related protocols used are disclosed to and understood/accepted by them.

6.4 Signalling

Rules relating to confirmation systems allow known loss of a signalling path to be treated by the ARC as, or contributing to, a confirmed activation in one of three ways during any period when I&HAS are known by the ARC to be set:

- known loss of a signalling path after an unconfirmed alarm activation;
- an unconfirmed alarm activation after known loss of a signalling path;
- known loss of two signalling paths within a 96-hour period.

To ensure all three eventualities are available to the ARC, all confirmation systems should be provided with dual path signalling, unless:

- the premises are in Scotland, there is no personal attack (PA) risk (see section 7) and the responding police force will still respond to known loss of a single communication path;

  or

- geographical considerations mean that no dual path signalling product can be found to work (in which case the best available single path solution should be used).

Note: Although use of single path signalling is permitted by DD 243, its weakness is recognised insofar as installers are required to include a warning about the effects of using it in their system design proposals.

See section 8.2 for further information on insurers' typical remote signalling requirements.

7. HOLD-UP (PERSONAL ATTACK) ALARMS

Hold-up alarms, usually referred to in the UK as personal attack (PA) alarms, can be stand-alone systems or, more usually, be incorporated within I&HAS. They are usually used to alert police, via an ARC, of the need for an emergency response to a series of events ranging from assault to robbery (theft with actual or threatened violence).

7.1 Personal attack facilities

PA facilities usually comprise a device connected to I&HAS which is activated by users pressing a double push switch, or which may involve the input of a special code to indicate duress when unsetting all or part of a system.

Note: The use of a 'duress code' to alert police is now restricted to Grade 4 systems, and, as a result, push button devices will be used at most premises where PA facilities are required.

• Is there a risk of an attack?

PA facilities can be an important feature of I&HAS, but because of the potential risks to users and the risks and resource implications to those responding (usually the police), they should only be proposed if a security risk assessment can demonstrate a real risk of an attack. The assessment should then outline the required type and best location for any PA devices, for example:

- use of double push (dual action) PA buttons, to prevent accidental activation; and
- siting additional PA buttons away from the immediate area where a robbery is expected to occur, possibly to allow for their safe use by persons viewing the scene of an attack but not directly involved.

Consideration should then be given to who is expected to respond, how quickly and how the request for response will be communicated. In a few cases, on-site security guards may respond, but in most cases a police response will be appropriate.

• Is there a risk of lost communication with the ARC?

Where a PA alarm utilises a telephone landline to transmit signals to an ARC, there may be a risk that this link could be cut prior to an attack, in an attempt to prevent transmission of any subsequent PA alarm signals.

As a result, a dual path telephone and radio-based signalling system should always be specified whenever a PA alarm is required, unless the risk of the line being cut can reasonably be considered negligible.

7.2 Intervention

Whilst new PA facilities are still accepted by the police, the problem of high numbers of false PA alarms has led to a tightening up of the numbers of false PA alarms that will be accepted before response is withdrawn.

Once response is withdrawn, the police generally wish to be convinced that robust measures have been taken to prevent further false calls before they will restore it. However, the ACPO Security Systems Policy (SSP) now calls for the compulsory use of intervention before response will be restored.

Intervention requires that, after a PA signal has been received, the ARC uses a recognised means of confirming whether it is likely to be a false alarm before requesting a police response.

There are currently three principal forms of intervention available to ARCs, which can be briefly summarised as:

- callback (ringback) – the ARC telephones the premises;
- audio – microphones transmit sound to the ARC; and
- visual – premises' cameras transmit images to the ARC.

Other methods of confirming PA alarms are under consideration.

Note: If the results of intervention are inconclusive – that is, contact with the site does not completely satisfy the ARC that all is well – the police can still be called.

• Is there a risk of using an inappropriate form of intervention?

Each of the three forms of intervention has various pros and cons associated with it, especially in terms of the safety of users.

Callback risks alerting the attacker to the fact that someone has used a panic alarm, whilst the use of audio intervention may not result in conclusive sounds being heard.

On balance, insurers are likely to favour visual intervention, which has several advantages, for example:

- silent operation;
- can confirm that an attack is underway and also provide good information for the police on the nature and number of attackers involved; and
- it may be possible to use parts of any existing CCTV equipment already installed.

8. ALARM SIGNALLING (NOTIFICATION)

To be effective, I&HAS need to provide a signal (referred to as notification in the Euro Standards) to alert someone to alarm activations/faults. This can sometimes be done by a local audible warning device (for example, a siren), ideally supplemented by visual strobe light indication, fitted at the premises. However, it is more reliably done by transmitting a suitable alarm message (signal) to another location, usually an ARC.

8.1 Local signalling – warning devices (WD)

In some cases, insurers will accept I&HAS provided only with local signalling – often referred to as audible only signalling (and which, in the context of the UK's adoption of Euro Standards, via PD 6662: **Scheme for the application of European Standards for intrusion and hold-up alarm systems**, is referred to as a Grade 2X system). Examples might include low risk premises where, when the alarm is likely to be set, someone is either living or working in part of, or adjacent to, those premises.

Note: 'Audible-only' signalling may occasionally be accepted by insurers at higher risk premises, for example, where an agreed level of appropriate manning – such as workers or site security guards – is always present when the alarm is set.

Even where remote signalling is required, insurers will usually still require at least one external self-actuating local audible WD to be installed, even if not described in the relevant grade notification requirements of the Euro Standards (see section 4), in an effort to deter or limit crime by:

- advertising the presence of an I&HAS;
- alerting intruders to the fact that they have been detected; and
- alerting neighbours or passers-by to any activation.

On occasions, a supplementary high intensity, mains-powered internal sounder, to disorientate intruders, may also be appropriate.

Note: A WD can also assist those responding, such as the police, in locating the premises. Those with a siren and strobe light can, where operation of the strobe light is delayed, also be used to alert keyholders called out to an unconfirmed alarm that it has subsequently become confirmed.

Audible warning devices should operate for the maximum time period permitted by the standards governing particular I&HAS – that is, 15 minutes for systems meeting the Euro Standards – or any lesser period imposed by national or local authority statute.

In addition, although permitted in the Euro Standards, insurers will not wish I&HAS to be programmed to allow the ARC to turn off a site WD after they have received an alarm activation.

• Is there a risk of intruders attacking a site WD?

Given the benefits of, or possibly reliance upon, a site WD, the risk should be considered that intruders may be able to gain access to it and seek to disable it, for example, by injecting quick-setting foam, smashing it or removing it from the wall.

Fig 4: The external WD should be sited out of easy reach

Where this is considered a possibility, particularly, for example, where it is not possible to install an external WD at least 4m above the ground (or 4m above any roof, or balcony, etc that is readily accessible from the ground), two external WDs should be fitted, sited, where possible, on different elevations of the premises.

• Is there a risk of intruders working undisturbed? (bell delay)

Intruders prefer to work in peace and quiet. To counter this, insurers generally want as much noise to be made on site as possible when an alarm system activates. In addition to possibly creating a local alarm response, this is likely to disorientate intruders and thus limit their activities.

Insurers will not wish to see a programmed delay in the operation of site WD (bell delay) except where remote signalling is provided and:

- a bell delay is required as part of any responding police force's SSP;

  or

- it is an audio confirmation system;

  or

- a personal attack device is activated.

Note: Wherever a bell delay is programmed, it must automatically be removed in the event of locally detected loss of all communications paths to the ARC.

8.2 Remote signalling – to alarm receiving centres (ARCs)

Other than at lower risk premises, as indicated in the first paragraph of 8.1, it is usual for insurers to require all I&HAS to have remotely monitored signalling – that is, a connection to a suitable alarm receiving centre.

In addition to recognising different notification permutations at each grade – that is, combinations of audible and remote single and dual path signalling – the Euro Standards set out progressively increasing grade requirements for various technical aspects of remote signalling, namely, signal transmission time, fault reporting time and the security of information.

Once geographic coverage and reliability have been considered then, other things being equal, fault reporting time is perhaps the most significant of these technical aspects to insurers; but a wide variation in fault reporting times is permitted grade by grade, as shown below for single path signalling coupled with a site WD (option B) and dual path signalling (option C):

- Grade 2:

  Notification Option B – 24 hours;

  Notification Option C – 24 hours on primary path, 24 hours on secondary path;

- Grade 3:

  Notification Option B – 5 hours;

  Notification Option C – 5 hours on primary path, 24 hours on secondary path; and

- Grade 4:

  Notification Option B – 3 minutes;

  Notification Option C – 3 minutes on primary path, 5 hours on secondary path.

The fault reporting times permitted for signalling systems within the Euro Standards can, in the context of known loss of a signalling path contributing to the generation of confirmed alarm activations, be inadequate in the UK and, in any event, are less than those insurers have traditionally been offered by some widely used

pre-Euro Standards remote signalling systems. Because of this, and other matters relating to interpretation of signalling requirements within the Euro Standards, insurers will, for the time being, tend to specify remote signalling by a brand and product of known performance, rather than merely specifying a generic grade and notification option.

• Is there a risk of signalling not working?

The UK telecommunications industry has numerous companies using different networks and technologies to provide their services. Access to some of these may be limited to certain population centres or, in the case of radio-based systems, have signal strength affected by local topography.

Certain alarm signalling products only work with designated telecommunications networks, or will not work (or may interfere with), certain types of telecommunications devices that a customer may use or depend upon. Expected availability – that is, the percentage of time over one year when the service is correctly operating – may also vary.

As such, installers should make checks on signalling coverage, radio signal strength and product-site compatibility before particular signalling products are proposed or used.

• Is there a risk of unreliability?

In addition to considering what signalling might work at a particular site, the risk of undue false alerts due to path failure should also receive consideration.

Whilst it is generally expected that loss of a signalling path will be detected promptly, the need to notify this to keyholders, who may then be required to attend the premises and investigate the cause and instigate remedial action under the terms of an insurance alarm condition, can create problems if it occurs spuriously and too often.

One possible measure of reliability is the signalling providers' stated availability. Availability is described in the Euro Standards but is not, as yet, a formal UK requirement. In respect of Grade 4 signalling systems, the Euro Standards require an availability level of 99.8% – that is, a maximum of 17.5 hours per year of non-availability.

In this regard, some forms of transmission may be more prone to poor availability than others, for example, radio signalling paths (especially at premises with weak signal strength) or IP signalling (where several practical and technical factors can lead to loss of broadband service). Single path IP signalling is likely to be particularly prone to numerous short duration outages and should therefore generally be avoided.

Separate RISCAuthority (formerly IPCRes) guides on IP signalling are available as a free download via www.riscauthority.co.uk.

Where availability information is provided (not all signalling providers can or will provide it), it should be considered in the context of avoiding undue false alerts. However, availability figures have to be considered with care as:

- they are inevitably based on past performance, so can only be generally predictive of the future; and
- the simple percentage figure may reflect numerous short duration faults (very likely to annoy a keyholder unduly called to investigate them) or a couple of periods of longer non-availability.

• Is there a risk of inadequately detected loss of communication with the ARC?

Where remote signalling is felt to be appropriate, it is important that loss of any communication path(s) between the premises and the ARC will be detected and notified to the ARC as soon as possible.

This means it is important that the signalling product used has prompt fault reporting on all paths, but especially on any secondary path once it is in sole use.

Fault reporting can be achieved in different ways. For single path systems, it requires some form of check (poll) signal being sent between the I&HAS and the signalling network and ARC, the absence of which indicates a possible problem and initiates further checking (polling*) prior to path loss being reported. For dual path systems, polling is also used, sometimes complemented by I&HAS signalling equipment monitoring the connection (interface*) between the two signalling paths, for example, looking for telephone line dial tone or radio signal strength, absence of which is noted and a suitable signal sent via the remaining path.

* Polling and interface monitoring are only a means by which fault reporting can be initiated, and as such should not be confused with the actual fault reporting time.

Although Euro Standards permit various grades of remote signalling, insurers will generally require remote signalling products that have fault reporting times at or near (see Note 2 below) Grade 4 requirements, that is:

- single path systems: within 3 minutes;

  or

- dual path systems: within 3 minutes for the primary path and within 5 hours (but ideally more frequently) on the secondary path – always subject to immediate checking of the remaining path once one has failed and suitable provision being made for step up on the secondary path (see Note 2 below).

Note 1: In accordance with the perceived level of risk, insurers will sometimes take a pragmatic view and accept signalling systems that have initial and/or 'stepped up' fault reporting intervals (slightly) less than Grade 4 requirements.

Note 2: If the primary path in a dual path system fails, insurers expect the secondary path to have its fault reporting time changed ('stepped up') to that which was required for the primary path, and that this enhanced fault reporting be maintained for a reasonable period. The Euro Standards are not explicit on how long this should be, so by implication it could be until the primary path is restored. However, on the assumption that a path loss has been reported, most providers start to reduce the fault reporting capability after a few days, often in an attempt to minimise any telecommunication charges involved.

Note 3: If remote signalling using internet protocol signalling (IP signalling) is proposed, the system should be designed to comply with either Level A (high risk) or Level B (ordinary risk) of the RISCAuthority (IPCRes) 'model' for IP alarm transmission systems.

Separate RISCAuthority (IPCRes) guides on IP signalling are available as a free download via www.riscauthority.co.uk.

• Is there a risk of local WD not being heard when the alarm is part set?

Where I&HAS are part set, it is usual for any remote signalling, excluding PA signals, to be disabled, and any activation of I&HAS to be limited to operation of any site WD.

This is based on the assumption that whilst part set, someone will be at the premises and be able to respond to any local warning device. In most cases, this will be the case, but not always. An example might be a large or noisy factory where some office areas are locked and remain alarmed on part set during a Saturday morning whilst work is undertaken in the process areas. In such circumstances, it is possible for a break-in to the alarmed office areas to occur and personnel on site might not hear the local warning device.

Where such a possibility exists, installing an internal warning device within the factory may be prudent.

9. ALARM RECEIVING CENTRES (ARCs)

Insurers usually expect remotely monitored I&HAS to send signals to a 24/7-manned alarm receiving centre which can, as appropriate, notify the alarm event(s) to keyholders or the police. In doing so, insurers need to be sure that such alarm systems are monitored in accordance with relevant British/European standards by knowledgeable and competent companies employing trustworthy personnel.

Because of this and police requirements for the issue of URNs, they will expect ARCs to have the relevant approval of a police-recognised, UKAS-accredited inspectorate – that is, the NSI or the SSAIB.

9.1 Procedures

I&HAS will only achieve the desired objectives if alarm-related messages are acted upon promptly by the ARC which, as appropriate, notifies them to keyholders and/or the police.

It is therefore important that ARC procedures for dealing with alarm activations, faults and other signalled events are transparent and in accord with what customers and their insurers might want and expect. They should therefore be set out in a formal response agreement and noted in adequate detail in the SDP and AFD documentation (see section 12.2).

Where ARC procedures do not match an insurer's expectations (see below), and the ARC will not change them to match, then the customer's attention should be drawn to this and a recommendation made that they consult their insurer.

• Is there a risk of ARC procedures delaying alarm response?

Most ARCs offer a standard contract setting out their terms of business and the usual services (response agreement) offered in respect of those I&HAS which are to be connected and monitored. Often the alarm user is only vaguely aware of what has been collectively agreed between their installer and the ARC used by them, which can lead to a shortfall between customer and/or insurer expectations and the service actually delivered.

Important note: Insurance policy alarm conditions will usually require keyholders to attend alarm protected premises as soon as possible after a reported alarm event/fault, and to not then leave them unattended until the alarm system is working in its entirety – including all means of communication with the ARC. *Without prompt keyholder notification, the intent of alarm conditions is undermined.* It is therefore important to insurers that ARC actions meet those set out above or are otherwise specifically agreed to by them. Installers may therefore consider it prudent to alert customers to this when recommending insurer comment on the proposed ARC and their usual operating procedures/response agreement.

Because of the desirability of somebody attending promptly and re-securing premises after any potential intrusion or damage, insurers expect an ARC to agree to notify keyholders immediately, or otherwise as soon as practical, of any signal received relating to:

- an unconfirmed alarm activation;
- a confirmed activation;
- an alarm, signalling or power system fault that does or could affect the ability of I&HAS to remain fully operational; or
- personal attack.

The ARC should also notify the police of qualifying activations as soon as the relevant rules permit them to do so – that is, in accordance with the type of system (non-confirmation or confirmation) and its status in relation to the responding police forces version of the ACPO (ACPOS in Scotland) SSP.

• Is there a risk of ARC procedures increasing the potential for a loss?

Where an ARC does not immediately notify keyholders of certain alarm events, they can create a potential for a larger loss than might otherwise be the case to occur. Examples of this include failure to report:

- an unconfirmed alarm activation until the system either generates a confirmed activation or fails to reinstate itself at expiry of the confirmation time (which can be set to between 30 and 60 minutes); and
- loss of one signalling path in a dual path system

The following scenarios illustrate the possible consequences.

Unconfirmed activations

ARCs are not aware of the precise extent of alarm coverage at the premises they monitor. Failure to inform keyholders of single alarm activations as they occur could mean that intruders are present in an area with, or leading to, target items covered by only one (or one working) alarm detection device. Without early keyholder intervention, this could result in one or more of the following:

- a sizeable loss if intruders restrict their activities to that area or use it as a launching point for a break-in to an adjacent one;
- more time for intruders to prepare a quick getaway, for example, by forcing open a larger door or moving a vehicle or more people into position;

- a forced open (alarmed) perimeter door being closed by intruders upon exit (allowing the alarm to reinstate itself upon expiry of the confirmation time) leaving the premises physically insecure, allowing the same, or other, intruders to enter later with ease; and
- extensive water damage due to rainwater ingress after forced entry, for example, has been made through a roof.

Dual path signalling

There are now numerous dual path signalling systems available to installers, each using varying methods of monitoring the integrity of primary and secondary signalling paths and reporting any failure at differing fault reporting times. Failure to inform keyholders of loss of a signalling path as it occurs could mean intruders can work undisturbed because:

- loss of the remaining signalling path is not reported at all, perhaps because the site equipment required to do so is smashed, or the remaining signalling path is disabled by, say, telephone line cutting or radio jamming;

  or

- loss of the remaining path is reported, but only some time after any incident has run its course.

10. RESPONSE ARRANGEMENTS

According to the assessed nature of the crime and safety risks at premises, appropriate arrangements need to be made to respond to all alarm activations/faults.

10.1 Police

Because of its potential timeliness, authority and back-up resources, insurers' default expectation is that alarm systems with remote signalling are, and remain, eligible for an immediate level 1 police response (or, where forces do not provide a level 1 response, the best available level) via the issue of a police unique reference number (URN). These are issued in accordance with the responding force's version of the ACPO (ACPOS in Scotland) Security Systems Policy (SSP).

Insurers will expect I&HAS designed for a police response unless:

- the nature of the premises to be protected or the type of I&HAS required precludes a police response – examples might include alarmed yards and compounds or temporary/portable alarms installed in empty buildings;

  or

- there is a low risk of significant loss – examples might include premises where there are no, or very low values of, target items present and no robbery risk;

  or

- there is a low risk of harm to the customer's keyholders – examples might include premises where the risk of intruder concealment is low, such as when the premises are compact and readily viewed externally and internally; or where a commercial response company acceptable to an insurer is contracted to attend, either instead of, or alongside, the customer's own keyholders.

Important note: It is vital that I&HAS without police response are sanctioned by any interested insurer. *Failure to do so may jeopardise insurance cover.* Installers may therefore consider it prudent to alert customers to this possibility when recommending insurer comment on types of I&HAS.

10.2 Non-commercial keyholders

As a result of police and insurer requirements, responsible persons (keyholders) need to be appointed by customers to attend alarmed premises promptly in response to all notified alarm activations and/or faults, in order that they can investigate the cause, allow others access – the police, for example – and then take any necessary remedial action before fully re-setting the alarm system and leaving the premises.

Provided they are suitably trained, comply with any insurance policy alarm condition that may apply and, if a police response alarm system, they reside within 20 minutes travel time of the premises, it is acceptable to insurers for keyholders to be premises or business owners, members of staff (sometimes called in-house keyholders) or friends or neighbours.

• Is there a risk of delayed or non-attendance?

Where non-commercial keyholders may not reliably attend, or cannot do so within a reasonable time window, the benefits of asking a commercial response company to attend, either alongside or instead of non-commercial keyholders, should be considered.

• Is there a risk of harm to keyholders?

Insurers' standard alarm conditions usually require a keyholder to promptly attend alarmed premises when advised by the ARC of any alarm activation/fault signal.

If the I&HAS is of a non-confirmation type with a URN, the police and a keyholder will usually be notified simultaneously, and hopefully attend together. In case this does not happen, keyholders should always be advised to:

- carry a mobile phone with them – and have it switched on;
- attend with someone else, whether another keyholder or a colleague or spouse/partner;
- take care upon arrival at the premises to survey the immediate scene; and
- call for police assistance via the 999 telephone system if there are clear signs of a break-in and/or intruders can be seen within.

However, if the I&HAS is of a confirmation type, then, depending on a number of factors, it could be that a keyholder is notified of an (unconfirmed) activation without the ARC being able to simultaneously request police attendance.

In such circumstances, a keyholder could find themselves attending premises with the possibility that an intruder may actually be present, with implications for keyholder safety. This risk should be brought to the attention of customers in the security risk assessment and steps taken to minimise it by:

- ensuring that sufficient/adequate detection exists to enable a confirmed activation to be generated as intruders enter the premises, rather than some time later;

- selecting a means of unsetting that does not allow intruders to enter and disable all confirmation or confirmation in at-risk areas;

  and

- ensuring that keyholders' mobile telephone numbers are held by an ARC – to enable them to attempt to inform keyholders of any unconfirmed activation that subsequently becomes confirmed;

  or

- programming a delay in operation of any WD strobe light, or fitting what is sometimes referred to as a confirmation indicator (an indication device fitted adjacent to the alarm entry-exit door to show whether or not I&HAS have registered a confirmed activation), the aim being to show a keyholder called out to an unconfirmed activation, and who is unable to be contacted en-route, that it has now become confirmed.

A separate RISCAuthority (IPCRes) guide **Electronic security systems – Selection and duties of keyholders** *is available as a free download via* www.riscauthority.co.uk.

10.3 Commercial keyholders

Insurers will usually accept use of commercial response companies that meet certain basic selection criteria, namely:

- the company holds NSI or SSAIB approval for their guarding/response activities;

  or

- the company complies with Security Industry Authority (SIA) requirements for licensed personnel – this is most readily ascertained by establishing that the company holds SIA Approved Contractor Scheme (ACS) status;

  and

- keys are not stored on site (see below);

  and

- for systems with police response, the company is able to meet expected police response times.

• Is there a risk of an intruder gaining access and turning off the alarm?

Some commercial response companies offer what they claim can be a quicker alarm response, by storing premises keys within a key box (key vault) attached to, or embedded in, the external wall of the premises in question, rather than keeping them at one of their operating bases or in a roving operational vehicle.

However, as confirmation alarm systems will require storage of the premises keys and an alarm operating device (keys or fobs) within the key box for response company use, the possibility exists that intruders may remove or open the box and then, using its contents, let themselves in and either turn off the alarm or otherwise turn off confirmation.

Insurers will not generally sanction site key storage, not least as it will be in clear violation of part of many standard intruder alarm condition wordings that typically require customers to:

- maintain secrecy of codes and security of keys and setting and unsetting devices for the operation of the intruder alarm system; and
- remove all keys and other setting and unsetting devices for the intruder alarm system when the premises are left unattended.

Insurers may on occasion, according to the perceived risk, accept the use of a key box if some additional risk specific security measures are adopted, for example, ARC monitoring of agreed premises and alarm opening and closing times and/or alarm protection of the key box itself.

Installers offering referrals to such services should therefore ensure that customers are aware of the security pitfalls this can present, and otherwise always recommend that they obtain specific insurer acceptance of the proposed arrangements, as per clause 6.9 of BS 7984: 2008: **Code of practice for keyholding and response services**.

Important note: It is vital that that the approval of interested insurers is sought when a commercial response company proposes storing premises keys and/or alarm operating devices on site. *Failure to do so may jeopardise insurance cover.* Installers may therefore consider it prudent to alert customers to this possibility when recommending insurer comment on proposed commercial response arrangements.

11. SECURITY FOG ('SMOKE') DEVICES

These devices, sometimes referred to as security smoke devices, are usually installed to supplement alarm protection, by temporarily preventing intruders seeing what it is they are trying to steal.

• Is there a risk of an alarm system failing to adequately prevent or reduce loss?

Given an adequate level of physical security, there can still be circumstances in which an I&HAS alone might not adequately control the theft risk – for example, where there is a risk of smash-and-grab style theft. In such cases, a security risk assessment could be used to indicate the need for a security fog device to complement I&HAS.

Insurers' typical requirements for security fog devices are that they:

- comply with BS 7939: **Smoke security devices: Code of practice for manufacture, installation and maintenance** (or its replacement BSEN 50131-8, when implemented in the UK);
- are installed and maintained by suitably trained NSI or SSAIB installers, with the design of complex systems involving the supplier's expert teams;
- are designed to take careful account of the need to activate at an appropriate moment during a raid, but equally, that they minimise the risk of false activations; and
- locally monitor loss of the mains power supply to the device and can notify this to the related I&HAS – from where it must be promptly signalled to the ARC (the heating block within the device required to generate the fog will cool without mains power).

A separate RISCAuthority (formerly IPCRes) guide **Security fog devices** *is available to view, or as a free download, via* www.riscauthority.co.uk.

12. DOCUMENTATION

Installers are required to document various aspects of I&HAS.

12.1 Risk assessments

Although they obviously need to be aware of its outcome, it is not a requirement that a customer be shown the installer's security risk assessment. However, most installers will disclose it, and many ask customers to sign it.

• Will customers understand the risk assessment?

Correctly handled, a risk assessment should be a positive aid to selling better I&HAS – that is, helping a customer understand why something is being proposed, rather than just considering the cost.

Therefore, rather than merely recording information, a risk assessment should also outline the security implications and impact of what has been assessed and recorded.

• Will insurers need to see the risk assessment?

Insurers, who in some cases are effectively the ultimate reason for a new I&HAS being installed, may not wish to see the alarm company's security risk assessment if it accords with the suggestions of their own underwriting guidelines or site visit.

However, providing a copy of the risk assessment to them may be helpful, particularly if seeking support for a course of action that is contrary to the insurer's usual or otherwise stated requirements.

12.2 I&HAS specifications

Various standards and alarm inspectorate rules require that alarm companies draw up documents detailing the nature and equipment used in I&HAS. Traditionally called alarm specifications, such documents are now correctly referred to as:

- proposed systems – system design proposal (SDP); and
- installed systems – as fitted document (AFD).

• Is there a risk of customers not understanding I&HAS documentation?

Most customers find a SDP or AFD, typically comprising a long list of detection equipment and their technical capabilities, very difficult to understand.

Consideration should therefore be given to providing a summary document outlining the areas in which cover is provided, and what the system is, and is not, designed to do in terms of the key issues of detection, fault reporting, tamper reporting, signalling and response.

There are not many premises where an alarm installer can adequately design I&HAS without using or drawing a plan, whether it be a simple sketch or one that is more detailed, for example, an architect's drawing. As most people more readily understand visual representations than wordy descriptions, a copy layout-detection plan given to a customer can be very helpful.

• Is there a risk of insurers not understanding I&HAS documentation?

Apart from the relatively limited number of staff an insurer may have with technical security skills, for example, security risk surveyors/ risk advisers, most of an insurer's other members of staff (such as underwriters) could have similar difficulties comprehending the intricacies of a SDP or AFD as would the alarm purchaser/user.

As a result, a simple summary along the lines mentioned above will benefit insurers. If this, or another document, provides clear details of ARC actions, for example, in event of signalling path loss and unconfirmed activations, etc, it will provide an insurer with a greater degree of confidence in the overall I&HAS arrangements.

In the same way, a copy layout-detection plan is an invaluable aid to an office-based insurer called upon to assess the design parameters and rationale of a proposed or already installed I&HAS.

Inevitably, whatever its other merits, the clearer the information provided to an insurer on the design of I&HAS, the more likely it is that installers systems will gain insurer approval.

Fire Protection Association
London Road, Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500 Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk

Hard copies of this document may be obtained from the publications department of the FPA at the above address.

Electronic copies may be obtained from www.riscauthority.co.uk.

Printed by: Information Press 07.09/3.0

RISCAuthority
formerly InFiReS

administered by
FPA
Fire Protection Association