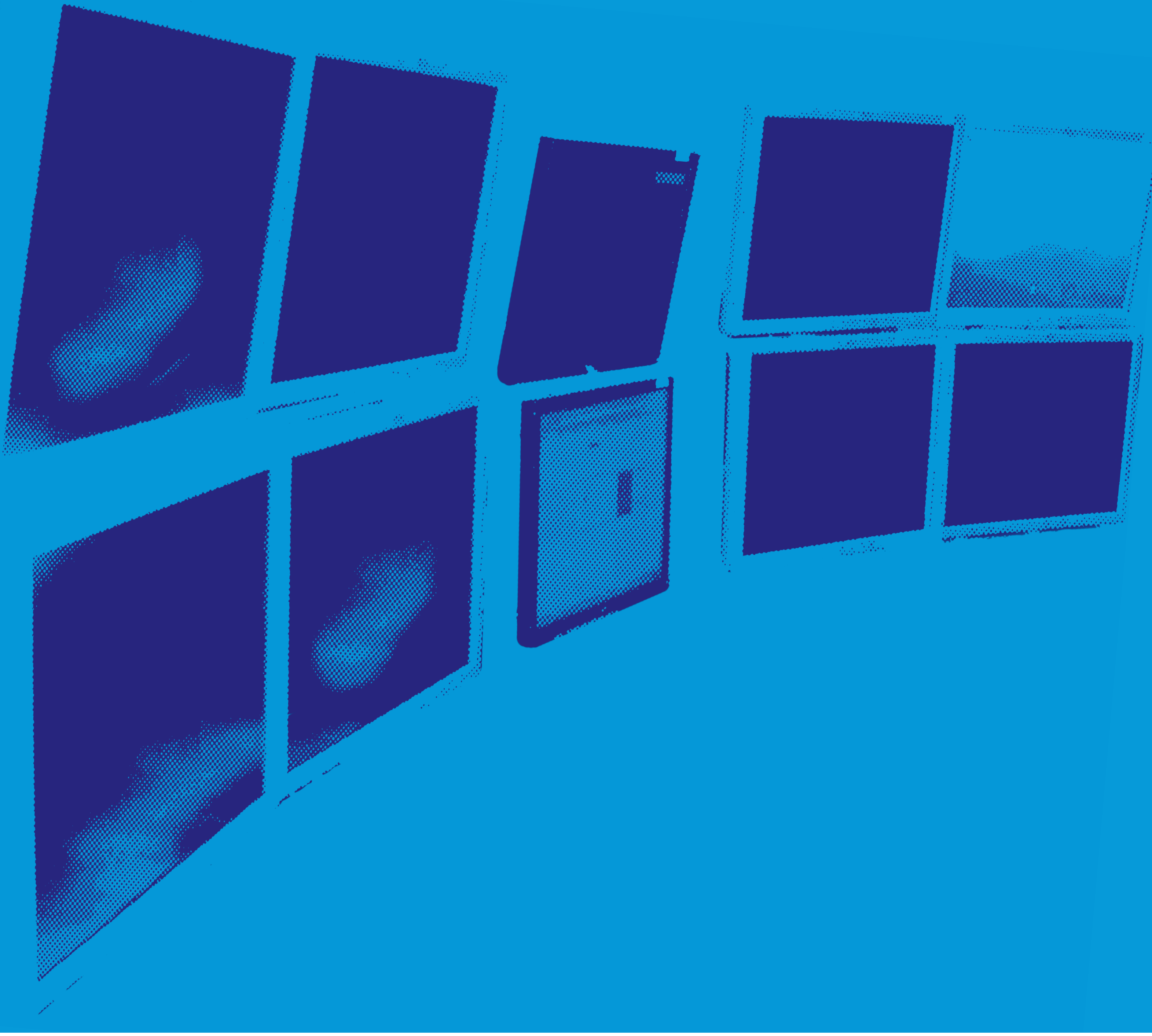
S17
First published 2011
Version 01

Security

Intrusion and hold-up alarm systems: guidance on event processing and handling



RISCAuthority

administered by FPA Fire Protection Association

IMPORTANT NOTICE

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

CONTENTS

1. INTRODUCTION

At a premises supervised by remotely monitored intrusion and hold-up alarm systems (I&HAS), various activations/conditions/changes of state ('events') recognised by such systems and/or their connected alarm transmission system (ATS) are likely to be fundamental to the security of those premises – most obviously because they indicate a possible criminal event, but also because they may indicate some failure or problem with the I&HAS/ATS themselves.

Signals relating to such events are usually transmitted to an alarm receiving centre (ARC) for handling by operators. The expectation is that all events that may be important for maintaining the security at a premises are presented to an ARC operator so that they can contact a nominated premises keyholder and, where appropriate and in accordance with the Association of Chief Police Officers (ACPO, or ACPOS in Scotland) rules, the police, who can then attend the premises and investigate the cause.

Whilst most events processed by the control and indicating equipment (CIE) of I&HAS, and transmitted by an ATS, are subject to specific provisions in British Standards, for example those in the BS EN 5013X: **Alarm systems** series, research conducted by RISCAuthority suggests that there is no generally accepted consensus on how all signals relating to such events are handled by an ARC.

As such, and also recognising that new technologies may increase both the number and extent of the information provided via such signals, there is an increasing risk of a mismatch between expectations and outcomes for the various parties who may be involved ('stakeholders'), which in turn may undermine confidence in the value of protection provided by I&HAS. This situation may be aggravated by the separation of, and possible poor coordination between, the three distinct provider groups involved, namely the alarm company, the ATS provider and the ARC, each of whom has different responsibilities as outlined below.

Notes

a) The key responsibilities considered to be borne by each of these groups in the context of this guide document are set out in more detail in the Appendix.

b) Various other documents relating to I&HAS and/or ATS, which may have relevance to those reading this guide, have been issued by the RISCAuthority:

- S2: **Alarm signalling using the internet protocol part 1: an overview**;
- S5: **Alarm signalling using the internet protocol part 2: considerations for insurers**;
- S6: **Electronic security systems: guidance on keyholder selection and duties**;
- S9: **Intrusion and hold-up alarm systems (I&HAS): considerations for installers and other stakeholders**;
- S12: **Police response intruder alarm systems: ten-step guide for purchasers**;
- S14: **Police response intruder alarm systems: summary of insurers' typical requirements**;
- S15: **Guidance on evaluating the performance of alarm transmission systems for use with intrusion and hold-up alarm systems**; and
- IPCRes guidance – **Security fog devices**.

(These documents may be downloaded free of charge from the website www.riscauthority.co.uk and those available in hard copy form may also be purchased from the Fire Protection Association.)

2. SCOPE

The information and recommendations contained in this document are primarily intended to guide the actions of alarm companies, alarm transmission system (ATS) providers and alarm receiving centres (ARC). The document will also be of relevance to other parties interested in the effective performance of intrusion and hold-up alarm systems such as customers ('end users'), non-installing specifiers (eg insurers), and regulatory bodies (eg alarm inspectorates).

3. THE ALARM COMPANY

The alarm company is responsible for ensuring that the control and indicating equipment (CIE) and ATS selected are capable of generating a full range of system alarm/fault events necessary for the efficient monitoring of the system and the security of the premises and personnel, and that these are appropriate for the risk assessed needs of their customer ('end user') and satisfy their expectations (and those of any interested third party, eg an insurer).

In order to conform to Annex G of the European Standard Application guidelines document (CLC/TS 50131-7), the customer must be given a system design proposal (SDP) document, which should include details of the main system functions and how key outputs will be actioned in terms of ARC responses (clause G12). However, the information actually appearing in these documents often leaves the reader in doubt as to the outcome of certain critical alarm system and ATS events, either because the information is missing/inadequate or because such information is not presented in a readily comprehended (standardised) format.

4. THE ATS PROVIDER

The ATS provider is responsible for ensuring that (as far as the extent of its control allows) the signals generated by the CIE and its connected ATS are reliably notified to the ARC in accordance with specified standards, specifications and codes of practice, and that, in addition, these satisfy its customers' expectations. In this respect, the ATS provider may regard its primary customer as the ARC (acting effectively as a wholesaler of their products) or the alarm company (effectively acting as a retailer), but, arguably, the end user should be regarded as its ultimate customer.

5. THE ARC

The ARC is responsible for ensuring that the events generated by I&HAS and any connected ATS are, when received by it, handled in a way that assures the efficient monitoring of such systems, the security of particular premises and personnel/keyholders, and that these satisfy its customers' expectations. In this respect, the ARC may regard its primary customer as the alarm company (acting as a wholesaler of their services to most of the alarm company's customers), but, as with ATS providers, arguably the end user should be regarded as its ultimate customer.

Of these three groups, the task of the ARC is commonly thought to be the most onerous/critical in relation to event handling, and there is certainly a case for seeing the ARC as carrying a heavy burden in maintaining the confidence of users and specifiers.

Responsibility for ensuring that outcomes match expectations rests with all three groups as indicated, but, as outlined above, the ATS provider and ARC may have a rather different perception of who their 'customer' is and what they may require by way of a standard or 'default' service. As such, in most cases, the alarm company has to take the primary accountability for setting up appropriate event handling arrangements and then ensuring, on behalf of end users, their adoption/continuity by the other two parties to any service agreement.

6. THE 'MODEL' TABLES

The RISCAuthority has prepared the guidance tables opposite to identify the key events that an informed end user, or other interested party, such as an insurer, would be likely to consider essential to the fundamental monitoring of I&HAS, and the related security and welfare of the protected premises, its occupants and keyholders.

These are tabulated and accompanied in each case with recommended or 'default' ARC handling actions. The tables are commended as a 'model' for monitoring in the generality of cases, but it is recognised that different event handling may be required for particular conditions. As an example, a formal agreement may exist (ideally with the acknowledgement of any interested party, eg an insurer) between the alarm company and the end user, whereby ATS fault signals are held at the ARC or within an ATS network/management centre pending receipt of further information/events, eg as part of the process for generating a 'confirmed alarm'.

Nonetheless, the intention is that all stakeholders in the process may find the model to be of use as a 'standardised template', and it is therefore offered to all interested parties for possible inclusion in any necessary agreements, system design proposals or other I&HAS related documentation.

It is hoped that the guidance assists in improving the transparency of the services under offer collectively from the three distinct provider groups discussed, and will thereby assist in the creation of a 'level playing field' of expectation that will benefit all interested parties.

Notes to the guide tables

1) The tables below provide a 'model' for the treatment of events to help the alarm company assure itself that all its systems, equipment and procedures, as well as those of the selected ATS provider and ARC with which it contracts (or otherwise instructs), align with the outcomes described. In the (unusual) event that the end user contracts separately or additionally with the ARC and/or the ATS provider, or if the ATS provider is appointed and instructed by the ARC, it is held to be the responsibility of the alarm company, as the applicant to the police for the unique reference number (URN), to ensure, as far as possible, that the performance of the ATS and ARC in combination meet the risk assessed needs of the end user as determined with the aid of this document.

2) The tables are largely designed to highlight the various events which should be notified to the police and nominated keyholders in respect of ACPO/ACPOS 'Type A' ('police calling') systems which have a current police URN, whether they are of an older type not recognised* as providing confirmed activations (non-confirmation system) or a modern type capable of providing confirmed activations (confirmation system). However, they can also be applied to ARC connected ACPO/ACPOS 'Type B' (non-police calling) systems, but in this regard (as type B systems are only intended to elicit a keyholder response, whether a commercial or non-commercial response), only the 'Keyholder notified' column applies.

3) *Account has been taken of the statement in the ACPO/ACPOS Security Systems policies that I&HAS installed prior to the implementation of DD 243: 2002: **Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice** but having a confirmation facility (ie installed at a time when confirmation technology was optional) are regarded by the police as non-confirmation systems. It is therefore assumed that ARC database and handling procedures in respect of police response have been so aligned, ie such systems will be treated by an ARC as a non-confirmation system.

4) It is also assumed that:

   a. The alarm system and the nature of signals transmitted to the ARC fully comply with relevant British and European standards, and police policy where applicable.

   b. The ARC conforms to BS 5979: 2007: **Remote centres receiving signals from fire and security systems. Code of practice** (irrespective of the possible withdrawal of BS 5979 by BSI, should that occur, and of any claim of conformance with any replacement standard that may be published by BSI).

   c. The events described are capable of being so designated by the alarm and signalling system, and then recognised as such by the ARC. Depending on the age/nature of a particular system it is recognised that some of the events may simply be transmitted as 'alarm' or 'fault'.

   d. Unless otherwise agreed in writing between the end user and the alarm company in advance of system commissioning (and subject to the procedures permitted in applicable standards), the events described in the tables are, on arrival at the ARC, always presented to the operator without delay and are then promptly passed to keyholders/police for action, as appropriate. Should this not be possible because of any limitation of the control equipment, and/or ATS and/or ARC technology, then this should be clearly set out in the system design proposal (SDP).

   e. If challenged by a keyholder as to the 'need' to attend site in response to a notified event, the ARC procedure would be to say that they are not in a position to advise. **Note:** To do otherwise would clearly not be prudent, as an ARC will not be aware of any implied or actual requirements on keyholders to attend. For example, those that may result from their employer's instructions or an insurer's policy conditions etc.

   f. A documented procedure exists in the ARC whereby attempts to contact a keyholder/customer continue to be made at pre-agreed prescribed intervals in the event that the initial attempt to do so fails. In exceptional circumstances, an ARC may determine that events received relating to an individual alarm system form part of a general catastrophic failure affecting a wide area or a particular ATS network, and, as such, whilst still being notified to a keyholder/customer, any normally necessary notification to the police may be unavoidably delayed.

7. A MODEL FOR CRITICAL EVENT HANDLING PROCEDURES AT AN ARC

I&HAS events (as presented to the ARC): SET PERIOD	Keyholder notified (all systems)	Police notified (non-confirmation systems with a current URN)	Police notified (confirmation systems with a current URN)
1.1 Alarm condition[1]	Yes	Yes	No
1.2 Confirmed alarm condition	Yes	N/A	Yes
1.3 Reinstatement with detector(s) inhibited	Yes	N/A	No
1.4 Expiring entry time	Yes	Yes	No
1.5 Tamper alarm condition	Yes	Yes	No
1.6 Hold-up[2]	Op	Yes[2]	Yes[2]
1.7 Duress[2]	Op	Yes[2]	Yes[2]
1.8 Prime power source failure (eg lost mains power)	Op[3]	No	No
1.9 Alternative power source fault[4] (eg battery low/failed)	Yes[5]	No	No
1.10 Any fault condition not otherwise identified	Yes	No	No
1.11 Deviation from agreed unsetting times, if monitored	Yes	No	No
1.12 **Single path ATS**: failure report (ie total ATS loss)	Yes	Yes	No[6]
1.13 **Dual path ATS**: first received path failure report[7] (ie partial ATS loss)	Yes	No	No
1.14 **Dual path ATS**: second received path failure report (ie total ATS loss)	Yes	Yes[8]	Yes[8]

Table 1: During the set period

I&HAS events (as presented to the ARC): UNSET PERIOD	Customer/ keyholder notified (all systems)	Police notified (non-confirmation systems with a current URN)	Police notified (confirmation systems with a current URN)
2.1 Tamper alarm condition	Yes	No	No
2.2 Hold-up[2]	Op	Yes[2]	Yes[2]
2.3 Duress[2]	Op	Yes[2]	Yes[2]
2.4 Prime power source failure (eg lost mains power)	Op[3]	No	No
2.5 Alternative power source fault[4] (eg battery low/failed)	Yes[5]	No	No
2.6 Any fault condition not otherwise identified	Yes	No	No
2.7 Deviation from agreed setting times, if monitored	Yes	No	No
2.8 ATS, all types: any failure report (ie whether partial or total ATS loss)	Yes	No	No

Table 2: During the unset period

(Op = optional)
See notes to the references [1-8] in these tables.

Notes to Tables 1 and 2

[1] For the purpose of these tables, an alarm condition is regarded as an event generated by an intrusion detection device or, where not separately identified (as per the tables), any tamper, masking or expiring entry time event, or any other fault event (affecting the security provided by the system), and which in all cases is either:

- generated as an alarm condition by a non-confirmation system; or
- generated as an unconfirmed alarm condition by a confirmation system*.

*__Important note:__ Where an alarm system incorporates sequential technology, keyholder notification should not be delayed pending expiry of any confirmation period.

[2] By way of clarification, both tables assume that hold-up/duress facilities remain operational on a permanent basis, ie whether any connected I&HAS are set or unset. In the case of systems that require confirmation (also sometimes referred to in this context as 'intervention') applied to hold-up alarm conditions, hold-up alarm/duress conditions are not to be passed to the police unless they are in compliance with ACPO/ACPOS Security Systems Policy and BS 8243.

[3] If the prime power source (PPS) fails, the alternative power source (APS) should be capable of running the system for some time, such that there may be no immediate need to notify a keyholder.

However, in certain cases* there may be a benefit in notifying a keyholder, eg where loss of the PPS could compromise other alarm, security or property protection facilities at the premises, in which case the alarm company should ensure that the ARC will take suitable action. Examples might include; a security fog system (its heating block will soon cool); an electronic lock/access control facility (it may 'fail safe' ie unlock); a CCTV system (it may cease to record images or suffer from absence of required artificial lighting); a stand-by generator (it may fail or need to be manually started) or the presence of refrigerators/freezers.

*__Important note:__ In this context, the alarm company should check that notification of loss of the PPS to the ARC is not being unduly delayed by the control equipment, ie being held on site for up to 1 hour, as permitted by BS EN 50131-1: 2006 + A1: 2009: **Alarm systems. Intrusion and hold-up systems. System requirements**.

[4] In relation to an APS fault, two distinct conditions may arise (of different immediate significance), but which are unlikely to be separately indicated to an ARC. One of these is 'low battery' – which usually indicates that the battery charge level (voltage) has dropped below a set threshold commensurate with its ability to run the system for the required period (as per the relevant governing standard) in the event of a PPS failure. Depending on when this occurs (in the battery discharge process), the system may still have a period of APS supply available. The other condition is 'battery failure', which could either occur due to continued discharge after a 'low battery' report or when the battery suddenly fails, eg equipment failure leading to a short circuit, etc. At this stage, the APS ceases to be operational.

[5] APS faults should be reported to a keyholder as from that moment, or shortly thereafter, the system may be relying solely upon its PPS. If the PPS subsequently fails and the APS failure report has not been reported to a keyholder, the only means by which the ARC might then become aware of a total power failure to a system would be if it subsequently received an ATS fault report (eg caused by local loss of power to the alarm transmission equipment) – the timeliness of which would vary according to the designed performance of the ATS. For example, an ATS performing at the ATS5 level could report such a fault within a few minutes, but lower performing ATS might not generate such a report for several/many hours, or not at all.

[6] 'Y' in Scotland where police have agreed to respond to loss of a single path and the ARC has been suitably notified of this agreement.

[7] The first path failure report emanating from a dual path ATS should be reported to a keyholder, as the ARC may not be a position to know the relative importance of the path lost (eg whether it is the primary or secondary path), nor the security adequacy of the background/enhanced monitoring of the integrity of a remaining path.

[8] Subject to second path loss being reported within 96 hours of first and within the same set period.

8. APPENDIX

This is a summary of the responsibilities of the alarm company, ATS provider and ARC in relation to event processing and handling.

The alarm company

- Carry out a risk assessment in accordance with DD CLC/TS 50131-7: 2010: **Alarm systems. Intrusion and hold-up systems. Application guidelines** and from this determine with the customer the alarm/fault events that the system will be required to generate including any processing/management procedures* critical to the interests of the customer.
- Select and suitably programme compatible control and indicating equipment (CIE). Arrange for compatible signalling to be provided by either selecting a suitable ATS or an ARC that takes responsibility for providing a compatible ATS.
- In undertaking the risk assessment, consider the risk of ATS attack/compromise by criminals and understand the claimed performance levels and related benefits/limitations of any ATS proposed, ideally seeking ATS products whose performance is independently validated (eg by third party certification/approval) to a suitable standard.
- Appoint a suitable ARC that contracts to respond to the alarm/fault events in accordance with the risk assessed needs of the end user.
- Document the above in the system design proposal (SDP) and as-fitted document (AFD).
- Maintain documented systems to monitor, as far as the powers of the alarm company allow, that the performance of the alarm system, complete with its ATS and ARC service, is sustained throughout the life of the contract to the agreed standard.

*In particular, ensuring that any ‘in house’ policy maintained by the ATS provider and/or the ARC for processing to be carried out (including any practice involving the ‘holding’ of certain types of signal at the ARC or within an ATS network/management centre pending receipt of further information) is made known to the end user and is compatible with their requirements, and is clearly documented in the SDP and/or AFD.

The ATS provider

- Ensure that the performance of the ATS is compatible/in accordance with the requirements of its customer (usually the alarm company but, where applicable, the ARC or the end customer) and that it meets any standard or specification with which conformance is claimed, including, if applicable, any requirements for ATS availability monitoring.
- Supply the alarm company with such information as is necessary to meet the recommendations in this document, in particular full details of any ‘holding’ of certain types of signals that may or may not occur and the precise circumstances under which such signals may be held and for what purpose.
- Make no changes to the agreed basis for any signal processing (including the ‘holding’ of signals within the ATS or its management centre pending receipt of further information) unless agreed in writing with their customer.
- Agree with its customer and other interested parties if appropriate, the action that will be taken in the event that developments arise outside the control of the ATS provider (eg technical problems at telecoms providers or possible criminal activity) that interfere, or are likely to interfere, with the agreed performance of the ATS.
- Maintain documented systems to monitor that the performance of the ATS is sustained throughout the life of the contract with its customer.

The ARC

- Ensure that the events generated by the alarm system and delivered by the ATS are handled in the manner directed by, or agreed with, its customer (normally the alarm company) whilst meeting any standard or specification with which conformance is claimed (including, if applicable, any agreed monitoring of ATS availability).
- Supply the alarm company with such information as is necessary to meet the recommendations in this document.
- Document, in agreement with the alarm company, the alarm/fault events that the system will be required to generate including the responses that will be made in each case and any agreed processing/management procedures – for simplicity, ideally utilising the RISCAuthority ‘model’ tables.
- Make no changes to the agreed manner of handling and management of alarm system events (including the ‘holding’ of signals pending receipt of further information) unless agreed in writing with its customer.
- Agree with its customer, and other interested parties if appropriate, the action that will be taken in the event that developments arise outside the control of the ARC (eg false alarm issues, technical problems at ATS/telecoms providers or possible criminal activity) that interfere, or are likely to interfere, with the agreed manner of handling and management of alarm system events.
- Collaborate actively with the end customer, alarm company and ATS provider to minimise false alarms in accordance with applicable standards, ACPO/ACPOS policy and industry best practice, and assist in the restoration of police response, where withdrawn, in accordance with those requirements and practices.

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.

RISCAuthority

administered by

FPA Fire Protection Association