S15
First published 2011
Version 01

Security

Guidance on evaluating the performance of alarm transmission systems for use with intrusion and hold-up alarm systems

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

GLOSSARY OF TERMS

Alarm confirmation

Configuration of an I&HAS whereby activation of two or more independent detectors (possibly also supported by visual images and/or audio signals) is required (giving confidence of there being a high probability that a genuine intrusion, or a genuine attempted intrusion, has taken place) before the (confirmed) alarm condition is extended to the responding authority (eg police).

AE

Annunciation equipment: Equipment located at an ARC which displays the alarm status of, or the changed alarm status of, I&HAS in response to the receipt of incoming alarm messages.

ARC

Alarm receiving centre: Continuously manned remote centre to which information concerning the status of one or more alarm systems is reported.

ATE

Alarm transmission equipment.

ATN

Alarm transmission network.

ATP

Alarm transmission path: The route an alarm message travels between an individual I&HAS and the associated ARC annunciation equipment.

ATS

Alarm transmission system: The chain of connected services and equipment, eg ATE, SPT, RCT, that enables alarm messages to travel between an individual I&HAS and the associated ARC annunciation equipment.

AVAILABILITY

Percentage of time (usually percentage/year) a system is functioning as expected (vis-a-vis 'downtime').

DP

Dual path: An ATS that uses two ATPs, each of different technology, eg landline and radio. Duplicate (two paths using same technology) or Additional paths may also exist.

GRADE

A performance level for an I&HAS as outlined in European Standards (BS EN 50131: **Alarm systems. Intrusion and hold-up systems** series). **Note:** *By association, a series of Grade-related Notification Options, each with varying ATS performance requirements, can result in reference being made to a 'grade' of remote signalling.*

I&HAS

Intrusion and hold-up alarm systems.

ISP

Internet service provider.

RCT

Receiving centre transceiver: ATE at the ARC including the interface to the annunciation equipment and the interface to one or more transmission networks, being part of an alarm transmission path.

SP

Single path: An ATS that uses one ATP.

SPT

Supervised premises transceiver: ATE at the supervised premises including the interface to the I&HAS and the interface to one or more transmission networks, being part of an ATS.

URN

Unique reference number.

1. INTRODUCTION

To be truly effective, intrusion and hold-up alarm systems (I&HAS) need to be able to reliably and promptly raise a human response to all critical events – whether related to criminal activity or system faults. Whilst on-site warning devices alone are sometimes sufficient to do this, it is more usual for alarmed premises to be, in addition, connected to an alarm receiving centre (ARC) remote from the premises. The ARC is able to notify designated keyholders and, in appropriate cases, the police – ie where I&HAS have a police unique reference number (URN) and the alarm event qualifies for police attendance under the terms of the force's security system policy (SSP) rules.

The connection between an I&HAS and an ARC is technically referred to as the alarm transmission system (ATS), but is commonly referred to as 'remote signalling'. As a crucial link in the overall security provided by an alarm system, its nature and performance, as well as any related ARC event handling procedures, are very important. Indeed, without suitable remote signalling, other typically important design aspects of I&HAS may have their intended effectiveness undermined.

In recent years, the advent of new police rules and alarm standards, coupled with new signalling technologies, has greatly increased the complexity of this issue. It has also spurred the development of many new remote alarm signalling products; many of which, whilst they help end users to reduce cost, offer variable security performance.

The current rules relating to remote signalling, the various operating methodologies of the numerous products now available, and the external impetus for changes to existing remote signalling arrangements all need to be fully understood for a complete grasp of the subject. This represents a challenge for all who may be involved, whether as:

- ATS designers (ATS providers/equipment manufacturers);
- those who routinely specify and install ATSs (alarm companies/installers);
- those who specify or otherwise provide advice on such matters (consultants/insurers), and for insurers especially where provision of insurance cover is dependant upon a defined level of I&HAS protection;
- those who monitor such systems (ARCs);
- those who may need to regulate/assess activity in this area (alarm inspectorates/certification bodies); or
- customers (end users) who pay for/rely upon the ATS fitted to their I&HAS.

Some of the current external incentives to review/change end users' existing remote signalling arrangements include:

- next generation networks (NGNs): the numerous currently installed digital communicators (digicoms) are likely to be affected by the implementation of NGN, the best known example of which is BT's '21CN' which involves the upgrade

of selected BT telephone exchanges to incorporate '21CN' technology. Even without NGN issues, it can be expected that alarm companies will increasingly wish to replace digicoms with other more sophisticated products. The general question that then arises is: 'what constitutes a technically superior (but still cost effective) general replacement for obsolescent digicoms'?

- 'swap outs': there appears to be a trend for alarm companies to offer end users ongoing cost savings based on using cheaper 'grade' 2 or 3 dual path products to replace existing 'grade' 4 single path products. Although the provision of a dual path product in replacement of a single path product is often simplistically positioned as a signalling 'upgrade', the question that arises is: 'are two paths always better than one?'
- internet protocol (IP) signalling: there is no denying that the world is 'going digital', with related use of the internet greatly expanding. This will increasingly affect the ATS market in terms of the number of providers offering remote signalling products and the variety of available products. Whilst IP signalling may have potential reliability (Availability) issues vis-a-vis 'traditional' signalling technologies, such that its successful adoption may best suit end users who have good IT control/infrastructure, the general question that arises is: 'do some of the claimed potential benefits of IP outweigh any perceived disadvantages?'

Note: *Alarm companies offering changes to installed remote signalling systems have a responsibility to alert end users to the need to consult their insurer, as failure of end users to notify their insurer of such changes could jeopardise their insurance cover, particularly if the 'grade'/performance of the alternative signalling product is less than that currently installed.*

2. SCOPE

It is important that end users are able to obtain a clear understanding from specifiers of the performance of the various signalling products and services now available, such that they can be sure that they do satisfy the risk assessed requirements for their personnel/property protection. Equally, it is vital that specifiers can knowledgeably and unambiguously obtain and provide suitable advice to end users, and in that regard that ATS providers understand what information and evidence of performance may be expected of them.

This document aims to assist this process by examining the technical issues seen as key to the dependable performance of an ATS, whether a 'traditional' ATS, or one of the 'new generation' systems now proliferating. It also offers advice on the potential for specifiers and end users to determine the assessed performance of ATSs via (independent) third party certification.

Remote signalling is usually seen as being of most importance to interested parties in the context of I&HAS that are eligible for police response, and this document's contents are therefore largely tailored to that end. However, the importance of remote signalling in the overall effectiveness of all remotely monitored I&HAS, and indeed remotely monitored CCTV systems, is such that its contents should be of general application.

Some of the issues discussed here are either mentioned in, or related to, issues raised in other documents (listed below) produced by the RISCAuthority (or its predecessor IPCRes). To avoid undue repetition of content, it is recommended reference is made to them in conjunction with this document.

- **Intruder alarms and a harmonised European Standard**;
- **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**;
- **Alarm signalling using the internet protocol Part1: An overview**;
- **Alarm signalling using the internet protocol Part 2: Considerations for insurers**; and
- Various Bulletins on 21CN and NGN (3) (available to RISCAuthority members only).

The various issues raised in this document have some of their roots in the long and varied history of remote signalling development, evaluation and specifier acceptance. Those who are less familiar with past remote signalling development, or who wish to refresh their knowledge, may find that reading Appendix A of this document – history of remote signalling technology and its evaluation, a useful first step to understanding the need for this document.

3. WHAT IS AN ALARM TRANSMISSION SYSTEM?

'Remote signalling' is technically referred to as an alarm transmission system (ATS). It typically involves a chain of connected component parts/services, for example:

- alarm transmission equipment (ATE) and the supervised premises transceiver (SPT). Devices located at the alarmed premises which can forward/receive alarm and fault signals to/from the RCT;
- alarm transmission network (ATN) equipment. This can be regarded as any item of equipment installed within the supervised premises through which signals between the ATE and the ATN pass;
- the alarm transmission network. This can be regarded as the telecommunications systems through which signals between the ATE and the RCT pass. Such signals may travel directly between the ATE and the destination RCT, via a mix of private and public networks, or via a combination of such networks and a signalling provider's 'managed network';
- the receiving centre transceiver (RCT). A device located at the ARC (supplied by the signalling provider) which can receive/forward alarm and fault signals from/to the ATE; and
- the annunciation equipment (AE). A device located at the ARC which displays information received from the RCT to an ARC operator.

In providing the connection between the ATE and RCT, an ATS will either use a single path (SP) or dual paths (DPs) for alarm transmission.

4. REMOTE SIGNALLING DEVELOPMENT

Over time, the type and performance of remote signalling has inevitably reflected available technology and the effect of external stimuli – for example the desire for secure signalling with quick fault report times, reduced false alarms and the development of intruder alarm standards.

An understanding of the current remote signalling scene is incomplete without a review of the history of remote signalling and how the market's acceptance of differing products and the companies providing them has developed.

This is more fully described in Appendix A, but, in brief, at one time the only practical choice for widescale remote signalling was the generic digital communicator (digicom). These simple devices were soon overshadowed by the arrival of proprietary ATS products which incorporated some form of checking of the signalling transmission path. These products were typically high profile brands that became widely recognised by specifiers and end users as providing better performance than a digicom. At the present time many new, as well as established, remote signalling providers are offering 'IP signalling' products that compete alongside 'traditional' products, so at this point it is worth considering what we mean by such terms.

Traditional signalling

Starting with digital communicators (digicoms), then moving on to single path telephone carrier technology and, more recently, dual path radio/digicom solutions, remote signalling has typically used standard telecommunications networks to transmit the necessary signals. This can be regarded as 'traditional' signalling technology.

IP signalling

IP signalling is a term generally recognised as applying to the use of the internet protocol (IP) for transmitting signals over telecommunications landlines. IP differs from 'traditional' signalling technology in a number of ways which may be unfamiliar to specifiers and end users. Furthermore, some of the companies providing IP products are likely to be relatively unknown.

The current challenge facing specifiers and end users, as signalling technologies and product variations develop, is the objective evaluation of ATS, whether they use traditional or new (IP) technologies.

5. WHAT IS REQUIRED OF REMOTE SIGNALLING PRODUCTS?

In assessing alarm signalling products, attention clearly needs to be paid to their intended/claimed adherence to relevant standards, eg European Standards (security 'grade' and notification option), and also their likely general effectiveness at the installed location, especially any problems that may arise due to perceived non-performance or poor reliability, eg successful criminal attacks or an undue incidence of transient path failure reports.

Excessive path failure reports are a particularly irksome matter to end users who require (or who are required to provide by, say, an insurer) a keyholder to attend the premises when informed by their ARC of any alarm event/signalling fault; especially as they may then be required to stay at the premises until the alarm system, including all its remote signalling, has been restored to full working order.

In short, an informed specifier or end user is likely to wish to use remote signalling products that:

- perform at a clearly understood level (ideally derived from a clear and unambiguous standard) suited to the desired level of security;
- are reliable, ie have good 'Availability' (that is have a low figure for percentage of 'downtime' each year);
- can quickly report path failure faults to the ARC, whilst avoiding undue false alerts; and
- are resilient to deliberate attack/interference or network problems.

5.1 Availability

The most frequently used measure of reliability is the percentage of time over a year that an ATS is working (available). ATS with poor Availability, perhaps due to numerous short-term service failures, could lead to keyholders being unduly called to attend premises many times in response.

The issue of Availability received significant attention in previous IPCRes documents on IP signalling where it was related to the possibility of more frequent non-Availability vis-a-vis 'traditional' ATSs. It was argued that this was partly to be attributed to the Availability of IP signalling being additionally affected by factors outside the ATS provider's, or alarm company's, control. For example, the quality of service provided by the end user's chosen Internet Service Provider (ISP), and the likely use (if potential cost savings are to be realised) of a 'shared use' IP network router at the end user's premises – both matters where the end user exercises ongoing control.

However, Availability is a potential problem for all signalling suppliers, whatever technology is used, so it would be unfair for IP signalling to be singled out in this regard.

Establishing Availability requires an ATS to be frequently checked for correct operation of its sole or primary and secondary paths. The more frequently an ATS is checked for possible failures (which may or may not be related to criminal attack), the more likely it is that transient faults will be detected. Therefore, to a certain extent, a compromise may have to be made between security and reliability.

Ultimately, end users are best placed to decide if they are being unduly troubled by unreliable remote signalling, and are likely to seek a change to another (more stable) product if they are unhappy with it.

5.2 Managed networks

When it comes to managing possible network problems, some account might reasonably be taken by specifiers of whether signals are sent via a 'managed network', that is one where a signal is delivered to, or monitored by, a 'management centre' of an ATS provider (who may undertake to ensure it reaches its ARC destination) or whether, in the absence of such a system, signals travel via 'point-to-point' transmission, that is entrusted to a public telecommunications network for delivery to the ARC, along with any other routine traffic being handled.

In addition to taking responsibility for message delivery, providers of managed networks may claim to provide other benefits to end users and alarm companies – for example, pinpointing the cause of faults, providing information about sites with intermittent connection issues, centralised password control (in connection with remote access to I&HAS) and the ability to review general alarm management information.

However, the ability of an ATS management centre to exercise control over some of the signals that are passed by the RCT to the ARC annunciation equipment (AE), and thus to an ARC operator, may also need to be recognised. This is especially so if a management centre is using this ability to control (hold) how and when certain alarm transmission path messages such as faults, are

presented to the ARC (eg to minimise false alarms). See section 7.7 of this guide, 'Can fault reporting reasonably be delayed'?

6. MATCHING SIGNALLING PRODUCTS TO RISK – THE PROBLEM

Familiarity with the performance of remote signalling products in the past, when there was only a very limited range of products available, was a fairly simple exercise. However, the advent of alarm confirmation and then the European Standards set new performance parameters. These in turn have led to an expansion in available products but, at the same time, many areas in the standards upon which such products are based are arguably incomplete or open to interpretation.

Indeed, back in 2005 the IPCRes guidance document on the then new European Standards recognised that the lack of clarity over some of their general and specific requirements could mean that generic identification by insurers of suitable ATS based solely on their claimed 'grade' would be problematic.

Since then, a significantly wider range of ATS providers and products have become available which, coupled with use of new/complex technologies and hard to verify performance claims, has made it all the more difficult for objective judgements to be made about which remote signalling product is best suited to different I&HAS applications.

This difficulty is exacerbated by the fact that old products exist alongside the new, and either may be encountered in association with a mix of non-confirmation and confirmation I&HAS, each of which may, or may not, also be subject to the grading system in the applicable standards.

This results in a situation where there are now around 30 different remote alarm signalling systems operating (either actively being sold or still in use) in the market; all of which are essentially doing the same thing, ie sending signals to an ARC, but in differing ways and with variable levels of performance, especially in terms of monitoring/fault reporting.

7. EUROPEAN STANDARDS BS EN 50131/ BS EN 50136 – UNRESOLVED ISSUES

Whilst much of the content of the European Standards relating to new intruder alarm systems and products are clear and widely regarded as uncontroversial, attempts to provide an objective baseline by which different signalling providers' products may be recognised are hindered, partly by the fact that the standards fail to fully deal with particular areas of interest to UK specifiers (eg in the context of confirmation I&HAS), and partly because in certain areas they are unclear.

An overview of the key technical features of the various European Standards is included in Appendix B; whilst Appendix C takes the form of a summary list of the key issues related to those standards, all of which are more fully discussed within the body of this guidance document.

Whilst all of the issues mentioned below, and elsewhere, do need full consideration by specifiers and end users, a key practical issue for both, but particularly end users, is reliably knowing when an ATS has partly or wholly failed. In this regard, interpretation of the relevant provisions of the European Standards is more straightforward for single path (SP) ATSs than dual path (DP) ATSs; with the former the ATS either is or is not operational, whereas with the latter one path may be working whilst the other is not.

For both SP and DP ATSs, some key issues that arise are outlined below.

7.1 What level of ATS Availability is appropriate?

ATS Availability, as originally prescribed in the draft BS EN 50131-1, was not incorporated in the published version. Accepting that there are difficulties in defining and reliably measuring Availability, some benchmark for the minimum amount of time an ATS can be expected to work is nonetheless generally desirable to help avoid end user inconvenience – not least as they may be required (for example, by an insurer) not to leave their premises unattended unless I&HAS (including the ATS) is fully operational.

7.2 Is ATS performance fixed or variable?

Some ATE can be set up by an installer to operate at various preset ATS 'grade' parameters but, that said, the initial set up should be evidenced in an alarm company's system design proposal (SDP) and as-fitted document (AFD), which should allow the specifier and end user requirements to be readily checked.

A potentially more problematic issue is that some ATSs can be remotely re-configured after installation to operate at a different performance 'grade'. There is no clear advice or protocol for alarm companies to follow for recording where such instructions may have originated, nor how end users should be advised to give their approval, eg accompanied by a suggestion that they check that any insurer or other interested party has been consulted about the proposed change.

For DP ATSs, some additional issues that arise are outlined below.

7.3 Does a DP ATS consist of one ATS or two?

Annex B provides more detail on the conflict between BS EN 50131 and BS EN 50136: **Alarm systems. Alarm transmission systems and equipment**, but in practical terms the UK intruder alarm industry appears to have made the interpretation that DP ATSs should involve one ATS with two paths, the primary path having to meet the main (higher) BS EN 50131 ATS performance values and the secondary path the additional (lower) ATS values. However, if the concept of one ATS with two paths is accepted then various questions arise:

- if the primary fails, should the secondary path take over its functions?;
- when the secondary path takes over, should its performance characteristics 'step up' to match the primary in all its performance aspects, or just some, for example the fault reporting requirement?;
- if a secondary path can meet all the performance requirements of the primary when operating in 'stepped up' mode, it would seem logical that it should also meet them (except for having a less frequent fault reporting time) whilst in stand by mode?; and
- do the fault reporting times shown against the 'main ATS' in BS EN 50131 relate to failure of the whole ATS (ie loss of both paths) or only the primary – to then be followed by the same (now stepped up) interval for any loss of the secondary? In practical terms, taking the former interpretation could mean that, for example at 'grade' 4, loss of both paths has to be reported in three minutes (increasing the possibility of generating undue false alerts, due, say, to short-term network failures). Taking the latter interpretation, such loss is reported after six minutes (a potentially significant delay in the event of a catastrophic ATS failure caused by criminal attack, for example entering a premises and destroying the ATE).

7.4 How should 'step up' be managed?

Accepting that when a secondary path 'steps up' it should perform as the primary, we then need to consider:

- what evidence is required that 'step up' has actually taken place? In other words, after loss of the primary path, should the ATS be able to check that the secondary path is operational; or can it passively wait for any possible loss of the (now assumed to be stepped up) secondary path to be reported only after the next scheduled fault reporting time interval passes?;
- if after loss of the primary path the secondary is checked for 'stepped up' operation, how quickly should a 'catastrophic failure' (effectively detected loss of the primary path followed by almost immediately detected absence of a working secondary path) take to be detected and reported?; and
- for how long should 'step up' operate? For a defined period of time or indefinitely (that is until the primary path again becomes operational)?

7.5 What level of ATS performance is appropriate?

Performance of ATSs is dealt with in the BS EN 50136 series, to which products may be tested, but when used in conjunction with I&HAS the 'grade' of signalling is partly dependent on additional equipment and performance requirements set out in BS EN 50131-1, some of which vary depending on whether an external Warning Device (WD) is fitted.

Note: *For DP systems an external WD is not required by the European Standards, so where one is required it should be separately specified.*

The actual level of ATS performance suitable for a particular end user should form part of an installer's security risk assessment – and in doing so the risk of ATS failure or compromise under attack, and its likely effect, should be borne in mind. In simple terms, there will either be a high or low security impact due to an ATS attack, with the following solutions likely to suggest themselves:

7.5.1 High impact

At premises where reliable and prompt notification of alarm signalling problems is considered essential to reduce the possibility of serious loss or damage, the level of performance of a 'grade' 4 DP ATS (three minutes primary path fault reporting) is likely to make it the 'default' choice of an informed specifier or end user; and especially when considered in the context of a police response (confirmation) alarm system.

7.5.2 Low impact

At premises where loss of signalling is considered less likely to have a significant impact on any criminal loss, an informed specifier or end user may consider a performance level lower than 'grade' 4 to be acceptable. However it is important to note that the current European Standard for 'grade' 3 has a minimum primary path fault reporting time of five hours and thus in the context of reporting faults that may arise from criminal activity, a wide gulf exists between the performance of 'grades' 3 and 4 (in recognition of this, a recent draft for the revision of EN 50136 proposes a revised fault reporting time of 30 minutes for a second tier DP ATS).

Moreover, with a primary path fault reporting time of five hours being widely recognised by ATS providers in the UK as inadequate, there are, in fact, significant differences in claimed levels of actual fault reporting performance between the various 'grade' 3 ATS products on the market. This tends to frustrate product assessment, comparison and selection on the part of the specifier and customer.

7.6 How should fault reporting be achieved?

Whilst the European Standards give maximum fault reporting times 'grade' by 'grade', and in dual path systems for both the primary and secondary paths, they do not state how this fault reporting should be determined. There are currently two methods by which it is done:

- the most reliable is by the ATS noticing the absence of some regular signal (poll) being sent between the ATE at the connected premises and the ARC. **Note:** *In the case of SP ATSs, fault reporting can only be achieved by this method*;
- when it comes to DP products the possibility exists for some, or all, of the fault monitoring to be undertaken within the ATE at the connected premises which, upon locally noting any fault in either of the two paths, could send a fault report via any remaining path. This method is less reliable than polling for two reasons:

  a) the ATE will usually be contained in, or be sited adjacent to, the I&HAS control panel. If this is in an area where it can be readily located and quickly destroyed by criminals, no alarm or path fault signals can be transmitted to the ARC. This situation is exacerbated where the I&HAS uses a means of unsetting that involves timed entry/exit and the ATE is installed within the zone designated as the entry/exit route. In this situation, criminals can exploit the period of (at least) 45 seconds that is allowed for entry (plus a possible further 30 second abort time) to carry out an attack on the control panel, before the panel can recognise that an intrusion event has occurred and try to send an appropriate alarm signal;

     Note: *Whilst BS EN 50131-7 contains some advice to installers on siting of control panels, this is not always fully appreciated and observed by installers, and it is not uncommon, particularly in pre-BS EN 5013X series systems, to find the control panel and ATE located within entry/exit route areas.*

  b) what is it that the ATE is checking? For example, is it basic radio signal strength, telephone line voltage, or the ability to actually make a call? And then, is that call made only to the nearest radio mast/phone exchange, or beyond that, e.g. to an ATS provider's managed network centre and/or the connected ARC?

Many DP signalling products use a mix of both methods, but ideally local monitoring should only be seen as a tool to help diagnose the location of a problem reported by polling failure. For example, whether a fault exists at the premises, between them and the local telephone exchange (or radio mast) or elsewhere.

Note: *Local monitoring may also be used to provide the required (under PD6662) local signalling path fault indications to users of I&HAS.*

7.7 Can fault reporting reasonably be delayed?

Whilst the fault reporting times mentioned in the standards obviously have to be observed by ATS providers, these are the maximum times that can pass before any fault is reported. As a transmission path failure report may relate to a short-term break in transmission capability, most ATS providers will, subject to the technology used, be checking transmission path integrity more

frequently than the 'grade'-related fault reporting time interval. This allows them to hold an initial fault report at the RCT, or within a managed network, whilst they check the transmission path again to see if service has resumed. If it has, an unnecessary ARC alert, perhaps leading to a keyholder call-out, can reasonably be avoided.

Once a path failure persists beyond the 'grade'-related fault reporting time, the European Standards require that the RCT generates a path failure report, but in this regard two further issues need to be considered, both of which stem from a desire to either avoid undue ARC traffic and/or false path failure reports being generated for keyholder action. These are:

7.7.1 Message 'holding'

Some ATS providers may take a view that in certain circumstances a transmission path failure report that persists beyond the 'grade'-related fault reporting time can reasonably be held by the RCT, or within their managed network, ie not passed to the ARC annunciation equipment (and thus an ARC operator), unless within the same set period of the alarm system an alarm condition has been reported beforehand, an alarm condition is reported subsequently, or a second path failure is reported (all of which would indicate a 'confirmed alarm' condition).

Note: *Such event 'holding' is a permissible practice in terms of DD 243:* ***Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice*** *(and its replacement BS 8243), as it allows for a written agreement from the end user to authorise such steps.*

The most significant effect of such a procedure is a scenario in which the first criminal attack on a premises involves the primary path being lost, say by an external phone line being cut, and intruders then enter the premises after the primary path fault reporting time has passed and 'step up' on the secondary path has commenced. If intruders can then reach the ATE within the connected premises without generating an alarm (this will depend on ATE location and alarm system design – see 7.6 above) and destroy the ATE, the earliest indication to the ARC that all ATS communication has been lost, will occur after the combined primary path fault reporting time and the 'stepped up' secondary path fault reporting time have expired.

The minimum delay will total six minutes (3+3) if the ATS is 'grade' 4 DP (but may be longer). If the ATS is a lower 'grade' DP system (with longer primary path fault reporting times) there will be a corresponding much longer, and potentially more significant, delay.

Any adverse effect of such a delay will usually be most relevant to general security risks, but could also delay attendance at premises which have been damaged/breached in some way (without an alarm activation being caused), such that rainwater can now freely enter and cause extensive damage or that arson may be facilitated.

In defence of this practice at all but higher risk sites, with a 'grade' 4 DP ATS the difference between a three minute keyholder-only response or a six minute keyholder + police response, may not have a big impact on the final outcome of a criminal event, and may in some cases have the benefit of avoiding (possibly lone) keyholder attendance at a site where criminals are waiting with duress in mind.

The key consideration for specifiers and end users in this regard is therefore ensuring that they know when event holding might be being proposed (it should be transparent and not implemented by default), and its possible adverse effect on early keyholder intervention at the premises. As such, specifiers and end users therefore need carefully to consider the merits and demerits of any proposed message holding, for example as part of an overall security risk assessment, and ideally one that is notified to any other interested party, eg an insurer.

7.7.2 Duplicate primary paths

Some ATS providers have products which have a duplicate primary path, that is one that is not normally in use but which can take over the functions of the primary path if that is lost. In such an eventuality, the ATS may arguably continue to provide the same level of overall protection as it did beforehand (it still has a primary path and a secondary path), and as such an unnecessary ARC alert, perhaps leading to a keyholder call-out, can reasonably be avoided.

The key considerations for specifiers with such products are, does the duplicate primary path 'kick in' before, or after, the primary path fault reporting time expires and, once in use, does it fully match all the required performance parameters of the lost primary path?

Whatever way any such 'holding' of path failures takes place, problems that have been recognised, but not acted upon during the set period, should be reported to the ARC or end user on the next working day or when the alarm is next unset – whichever is the sooner – to allow for possible remedial action to be taken.

Note: *ARC alarm and signalling event handling forms part of a separate strand of current RISCAuthority activity.*

8. ATS CERTIFICATION

All of the aforementioned issues relating to lack of clarity in the standards/rules assume greater significance where ATS providers 'self certify' compliance with those standards/rules, as specifiers and end users will not readily and reliably know upon what ATS features providers have based their self certification. In addition, by the very nature of self certification, specifiers will not readily be aware of the nature of any testing regime that has been undertaken.

For these reasons many specifiers and end users support third party (independent) certification, with a visible and clearly understood methodology (that is without potential confusion or uncertainty over the nature and testing of key performance parameters) to improve the confidence that can be had in any ATS performance claims.

The limitations and imprecision of certain aspects of the European Standards currently in force have already been discussed. However, it has to be acknowledged that such standards are created to be of general application across Europe, and, as such, can realistically only provide a baseline standard. Within individual European states additional requirements may be deemed necessary (this is recognised in the official European 'interpretation document' to EN50131-1) provided they do not conflict with the European Standards. The RISCAuthority Security Group maintains a watching brief over this important area and will report any developments impacting the standards and certification scene here in the UK.

9. CONCLUSION

Remote signalling is an aspect of electronic security system protection that has recently grown markedly in complexity, prompted by the emergence of a number of developments:

- alarm confirmation and its related need for dual path signalling;
- a widening range of new, fiercely competing, ATS products on the market;
- use of new technologies, with contested claims as to their effectiveness;
- unsatisfactory European Standards, some in transition;
- ATS performance claims that are difficult to verify;
- 'next generation networks';
- 'managed' ATSs and/or networks; and
- absence of suitably comprehensive schemes for independent ATS certification.

Ideally, most, if not all, of the issues outlined in this guidance document could in due course be tackled and resolved by revised EN Standards, or possibly new British Standards, with performance then assessed by suitable certification bodies and with related installation practice forming part of intruder alarm inspectorate audits.

In the interim, the job of the specifier or end user in selecting an ATS type that matches the (risk assessed) need in a particular situation is far more challenging than at the time when there might have been just one or two generic or proprietary systems available.

This guidance document has therefore attempted to identify the key issues that all interested parties need to take into account before making decisions about ATSs. As is hopefully evident, such decisions cannot adequately be made without investing some time in fully considering this complex and important topic.

APPENDIX A: HISTORY OF REMOTE SIGNALLING TECHNOLOGY AND ITS EVALUATION

Although a few '999 dialler machines' and 'DC leased lines' between alarm protected premises and emergency control rooms/police premises had been in use beforehand, remote signalling systems only began to become widespread with the advent of the digital communicator (digicom) during the 1960/70s. These relatively simple and robust pieces of alarm transmission equipment (ATE) were generic devices (made by several manufacturers) and simply connected to an available PSTN telephone line.

Subject to the 'phone line being available, ie not being blocked or cut, on activation of I&HAS a digicom 'dials up' its programmed ARC and, on connection, quickly transmits a coded message. To prevent criminals 'dialling in' to the connected 'phone line (so that they could let it ring continuously and thus block the digicom from making outgoing alarm calls), most high risk sites originally had digicoms connected to a separate ex-directory incoming calls barred (ICCB) phone line.

Thieves soon realised that cutting telephone lines and waiting to see what, if anything, happened next was an easier way of compromising alarm signalling than 'dialling in'. This is because when a phone line to which a digicom is connected is cut, the ARC would typically be unaware of the loss of the communication link (transmission path) – meaning that the connected alarm system cannot send any signals should a break-in subsequently take place. Partly as a result of these criminal tactics, the practice of using ICCB lines with digicoms fell away over the years, a trend accelerated by the introduction of modernised telephone exchanges that would cut off incoming calls that were not answered within a short space of time.

Apart from a very few heavy security risks that had their own leased telephone line between the protected premises and an alarm company's central station (ie an ARC), an expensive solution rather prone to intermittent faults, for many years digicoms were the only realistic option available for most insured risks. As such they were widely specified by the industry and insurers and, despite their potential weaknesses (chief of which was that the signalling was not 'monitored' as were leased line connections), thousands of them remain in use today.

A cost effective solution to digicom weakness was available for a relatively short period spanning the 1970s and 1980s, when many alarm companies acquired or developed 'multiplex' technology which allowed multiple sites to share a single telephone circuit or network and enjoy 'monitored' signalling.

However, the capital and line rental costs were such that alarm company controlled multiplexed networks could not compete with a new proprietary ATS that used the existing telephone service in the protected premises as a medium for its 'carrier signals'. This was branded in the UK as British Telecom 'Red' (later 'BT Redcare'), which was rolled out across the country progressively starting in the late 1970s. This service saw a continuous inaudible 'tone' transmitted over the telephone lines between BT's Redcare network and connected alarm systems, such that loss of the transmission path was quickly detected (typically within 1 minute) and notified to the ARC.

In this way, for the first time on a near national basis, a 'monitored' signalling service was provided without the need for an additional dedicated line. This was important because at that time, police forces would treat any detected transmission path failure (fault report) from I&HAS with a URN as a full alarm and attend the premises. As alarms could also be sent if the telephone line was in use, the provision of a separate ICCB telephone line to prevent 'dialling in' was also unnecessary.

Later, packet switch radio networks were established in the UK, and for some years one manufacturer marketed a single path ATS using a commercial packet switch network as the medium. In course of time, this was developed into a dual path product that used a digicom as the additional path.

By the mid-1990s, the number of false alarms being passed to the police, including 'line faults' had started to cause concern, and ACPO indicated their desire for the alarm industry to start to consider designing systems that could generate confirmed alarm signals. In this context the detected loss of a single transmission path is not helpful if there is no second path over which any subsequent alarm signals can be transmitted. It was partly in response to this new dimension that dual path products were launched in the market.

At that stage, there were still no specific UK rules dealing with the design of DP signalling systems, although the draft European Standards were known and available. However, when ACPO decided that URNs would only be issued for new I&HAS if they were 'confirmation systems', the impetus to develop an appropriate confirmation standard, which also dealt with the general nature and handling of outputs from signalling systems, was realised by the issue of British Standard Draft for Development DD 243: 2002.

DD 243 required that each path in a DP ATS must use different technologies, eg radio and telephone line, and allowed an ARC to request police attendance where detected loss of two transmission paths occurred. It therefore became important that each path was capable of being monitored for loss, and that path loss on both could be quickly and reliably detected. With reference to the coming European Standards this was known as 'Fault Reporting' (FR). Fault Reporting on what became known as the 'primary' (main) path is usually superior (ie faults are recognised more quickly) than that on the 'secondary' (standby or normally redundant) path.

The concept of a primary and secondary path, with different FR times, raised the issue of 'step up', i.e. the ability of the secondary path to improve its performance to match that of the primary path once the primary path fails. In the expectation that single path faults would still be reported by an ARC to keyholders, most DP products offered 'step up' performance that only lasted for a few days – typically based on an expected business break over a weekend, after which the stepped up fault reporting times started to decrease before reverting to normal.

The 2004 version of DD 243 introduced a requirement that second path failure, after detected loss of the primary path, could only be regarded as a confirmed signalling failure if it occurred within 96 hours of the first reported loss from I&HAS and during the same set period – this being based on an expected maximum four-day business break, eg an Easter bank holiday weekend.

The formal introduction of European alarm standards to the UK in 2005 led to I&HAS having to be Graded. Inevitably, their related remote signalling systems similarly came to be referred to as 'graded' too, but technically no Grades of signalling exist – see Appendix B.

At this time, the few DP products that had already become established were generally accepted as performing at, or close to, 'grade' 4 signalling performance. However, ATS providers seeing the range of ATS 'grades' set out within the standards started to develop 'grade' 2 and 3 signalling products, with many installers inevitably using them to match the Grade (2 or 3) of installed I&HAS. In doing so, they were perhaps not always fully appreciative of the possibility, and indeed desirability, of treating Grade of the alarm system and the 'grade' of remote signalling as separate matters.

Stemming from this demand grew for the ability to upgrade already installed signalling systems and this partly led to signalling suppliers developing products capable of having their installed performance retrospectively changed from one 'grade' to another.

Latterly, as broadband internet connections have become widespread in the UK, several new players have entered the UK alarm signalling market. Their products generally have an internet protocol (IP) based primary path and (typically) a radio (GPRS) secondary path. As these new systems became available the RISCAuthority Security Group (formerly IPCRes) issued two guides on IP signalling. These guides sought to explain the new technology and discuss some of its potential benefits and its possible pitfalls.

Some of the issues discussed in the IP part 2 guide are expected to be overtaken by new European Standards currently being prepared. For example, it is expected that any device at the supervised premises that is connected between the ATE and the external connection to the network used to transmit messages, eg an end user's 'shared use router' will be defined as 'network equipment' and not ATE.

Putting the 'shared use' router issue aside, some of the other issues raised in the IPCRes guides on IP signalling remain concerns for specifiers and end users to resolve. On the other hand there are other concerns in connection with the use of IP that are now arguably lessened through experience (many such systems are now being used by corporate businesses) and the exchange of information between interested parties. In short, IP signalling, and the various views concerning it, remains a developing area.

APPENDIX B: EUROPEAN STANDARDS

The general and specific requirements for remote alarm signalling are to be found in two main European Standards, which were originated at different times in different working groups. Unfortunately there is a lack of cohesion between them in some areas and in others they are ambiguous or arguably incomplete.

These documents are part of the BS EN 50136 and 50131 series, and are:

- BS EN 50136-1: **Alarm systems. Alarm transmission systems and equipment**; and
- BS EN 50131-1: **Alarm systems. Intrusion and hold up systems**.

A brief resume of their main features (and for 50131 only vis-a-vis signalling) is provided below.

BS EN 50136-1

Describes various performance criteria for different aspects of an ATS and provides benchmarks by which they can be assessed. The main areas dealt with include:

- average transmission time (D) – how quickly alarm messages can usually be sent;
- maximum alarm transmission time (M) – what the maximum permissible time taken to send a message is;
- reporting time (T) – how quickly any transmission path fault is reported;
- substitution security (S) – how well the ATS is able to detect that components may have been substituted by others;
- information security (I) – what level of encryption is provided to transmitted messages; and
- Availability (A) – what proportion of a 12-month period the ATS is fully operational.

Of these features, all other things being equal, arguably the most significant are the fault reporting time (T) and ATS Availability (A), as by these two criteria the general security and reliability of an ATS are most easily judged.

Notes:

1. *50136-1 mentions the possibility of an ATS having an additional (normally redundant) path, but only as a means to assist the 'Availability' requirements. The concept of 'step up' is alluded to insofar as this redundant path can perform at a lower set of ATS criteria when it is not in use.*
2. *Availability requirements were not included in the UK adopted version of BSEN 50131-1.*

BS EN 50131-1

Deals with I&HAS security grading, and on the subject of signalling (referred to as 'Notification') contains an important table (Table 10) showing four Grades of I&HAS and a range of notification 'options' (A, B, C or D) for any given one of them which relate to permutations of:

- the number and type of warning devices (site sounder) ranging from zero to one (battery backed up) WD or two (remotely powered) WDs;
- the number of ATSs, ranging from zero to one or two (a 'main' and 'additional' ATSs); and
- a minimum 'performance criteria' for the ATS(s) as outlined in Table 11 of the standard.

Note: *BS EN 50131-1 mentions 'main' and 'additional' ATS without clearly defining how this can be achieved. The UK intruder alarm industry has in effect taken the stated need for two ATSs to mean one ATS with two alarm transmission paths (dual path ATSs), with each path performing as per the separate ATS values of Table 10 and designated, accordingly, as the primary and secondary paths.*

Although there are no 'grades' of signalling, just a series of notification options with performance requirements that increase as the Grade of I&HAS they are to be used with increases, the UK alarm industry is in the habit of referring to 'grades' of signalling. However, even then it can be seen that referring to 'grade' 4 signalling alone is simplistic and incomplete, as within that 'grade' there are varying ATS performance options available according to whether or not a warning device (WD) or additional ATS (path) is used. What is additionally needed is some reference to the relevant notification option. This means that a specifier/end user proposing to use a 'grade' 4 dual path ATS, for example, should technically ask for an ATS that is suitable for use with a Grade 4 I&HAS at Notification Option C, and if required separately specify an external warning device. Clearly, this doesn't trip off the tongue, which is probably why reference to 'grades' of single path and dual path signalling has become commonplace.

The fact that Table 10 of BS EN 50131-1 contains the requirements for four Grades of alarm system (detection and control/indicating equipment), and for each of them four notification options, might suggest that for any Grade of alarm system only the signalling notification options shown beneath it can be used. However, there is no part of the standard that states this. It therefore appears that, subject to the 'grade' related notification option matching a set of ATS values equal to or greater than those called up in Table 10 by virtue of the Grade of I&HAS, the specifier is free to select the Grade of I&HAS and a 'grade' related ATS notification option independently, that is for optimum compatibility with the demands of their site risk assessment.

It is noticeable in the context of custom, practice and specifying conventions in the UK, that application of these ATS 'grades' without qualification has implications for whether a local warning device is, or is not, included.

In the context of the products available in this market it is also noticeable that the current standards do not state unequivocally that 'step up' has to take place – ie that the fault reporting time of the secondary path must 'step up' to that of the primary when the latter has failed. There is also no requirement that each path in a DP ATS uses different transmission technologies, as might be required in confirmation I&HAS installed as per DD 243/BS 8243.

Table 11 (see opposite) of BS EN 50131 helps further explain Table 10 as it shows, for each ATS value shown in Table 10, ie ATS1-ATS6 (with 6 being the highest), what performance parameters are required for each individual ATS component as described in BS EN 50136-1, that is values for D, M, T, S, and I. These ATS numbers (with related performance times taken from 50136 added in brackets) are shown opposite.

Table 10 from BSEN 50131-1

Notification equipment	Grade 1			Grade 2				Grade 3				Grade 4			
	Options			Options				Options				Options			
	A	B	C	A	B	C	D	A	B	C	D	A	B	C	D
Remotely powered audible WD	2	Op	Op	2	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op	Op
Self-powered audible WD	Op	1	Op	Op	1	Op	Op	Op	1	Op	Op	Op	1	Op	Op
Main ATS	Op	Op	ATS 1	ATS 2	ATS 2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6
Additional ATS	Op	Op	Op	Op	Op	ATS 1	Op	Op	Op	ATS 3	Op	Op	Op	ATS 4	Op

Note 1: *The single numbers specified for WD give the number of audible WD required for each option.*
Note 2: *ATS1, ATS2, etc refer to the performance criteria specified in Table 11.*
Key: Shaded areas = Optional

Table 11 from BSEN 50131-1

Performance criteria	Transmission time classification	Transmission time maximum values	Reporting time classification	Substitution security	Information security
ATS 1	D1 (120s)	M1 (480s)	T2 (25hr)	S0	I0
ATS 2	D2 (60s)	M2 (120s)	T2 (25hr)	S0	I0
ATS 3	D2 (60s)	M2 (120s)	T2 (25hr)	S1	I1
ATS 4	D2 (60s)	M2 (120s)	T3 (300min)	S1	I2
ATS 5	D3 (20s)	M3 (60s)	T4 (180s)	S2	I3
ATS 6	D4 (10s)	M4 (20s)	T6 (20s)	S2	I3

APPENDIX C: SUMMARY OF BS/EN ISSUES OUTLINED IN THIS GUIDANCE DOCUMENT

These are matters which specifiers may consider important, particularly in the context of ATSs used in conjunction with UK installed police response I&HAS.

- Should a level of ATS Availability be required?
- Are claims of the percentage of time that an ATS is available based only the period an associated alarm system is set or on the combined period of set and unset states?
- Is a dual path ATS one with two different ATSs, or one ATS with two paths?
- In a DP ATS should the 'main ATS' fault reporting time be taken as applying to the whole ATS or the primary path only?
- If an ATS has two paths, should the secondary path:
  - o be capable of fully matching (stepping up) its performance level to match that of the primary once the primary is lost?
  - o be permitted to have a longer fault reporting time when in stand by mode?
  - o be actively checked for correct operation immediately upon loss of the primary, or be passively assumed to be operational pending expiry of the 'stepped up' fault reporting time?
  - o be able, through immediate checking within a defined short period, to quickly contribute to a designation of catastrophic (total) ATS failure?
  - o have a defined period of operation in 'stepped up' mode?
- If a duplicate primary path exists should it:
  - o be capable of fully matching the performance level of the primary once the primary is lost?
  - o require any background checks when not in use?
  - o be checked for correct operation immediately upon loss of the primary, and if so within or outside the primary path fault reporting time?
  - o have a defined period of operation when in use?
- If the fault reporting times of an EN 'grade' 3 DP ATS are not generally considered adequate, what alternative figure should be followed?
- Should fault reporting times of each path to be determined by end to end polling or site ATE?
- Are key aspects of ATE fitting instructions and ATS configuration parameters suitably drawn to installers' attention?
- Is sufficient advice given to installers on identifying and protecting site network equipment?
- What protocols exist to ensure ATE/ATSs with variable performance parameters are :
  - o provided in a recognised ('grade') default configuration?
  - o suitably authorised by end users if set up by installers differently to the default, or later changed from it?
- What protocols exist to ensure that ATS messages are immediately passed to the ARC AE, and thus an operator for action?

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