



IPCRes **guidance**

InFiReS
Insurers' Fire Research Strategy funding scheme

Alarm signalling using the internet protocol Part 2: Considerations for insurers



Fire Protection Association
Protecting people and property

London Road
Moreton in Marsh
Gloucestershire GL56 0RH

Insurers' Property Crime Research (IPCRes) working group

This guidance document has been developed by the IPCRes working group of InFiReS (see below). IPCRes publications continue the tradition of providing authoritative guidance on crime prevention topics which was established by the Crime Panel of the Association of British Insurers.

Important notice

This document has been developed through the Insurers' Fire Research Strategy scheme (InFiReS) and published by the Fire Protection Association (FPA). InFiReS 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 InFiReS Steering 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 have 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 make 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 make 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.

First published by

The Fire Protection Association

London Road

Moreton in Marsh

Gloucestershire GL56 0RH

Tel: +44 (0)1608 812 500, Fax: +44 (0)1608 812 501

E-mail: sales@thefpa.co.uk, Website: www.thefpa.co.uk

2007 © The Fire Protection Association for InFiReS ISBN 1-902790 44-8

Copies of this document may be obtained from the publications department of the FPA, at the above address, or by calling +44 (0)1608 812 500 or e-mailing sales@thefpa.co.uk.

Printed in Great Britain by Modern Colour Solutions. 2.0/4.07

Contents

Purpose and scope	4
Today's signalling scene	4
The impact of IP	5
The impact on IP signalling of systems and equipment standards	6
IP systems contrasted with other systems	7
Summary	12
Conclusion	14
Appendix 1: Insurers' model for IP-based alarm signalling systems	15
Appendix 2: Overview and comparison table of signalling methods	17
Abbreviations/Glossary	18

1. Purpose and scope

Alarm signalling using the internet protocol: Part 1: An overview provided a review of alarm signalling using the internet protocol (IP). This second document considers the issues for insurers that are emerging with the introduction of this technology, and proposes a basis for evaluating the various implementations of the technology.

Specifically, the purpose of this guide is to help the insurance industry assess whether IP-based alarm transmission systems (ATSS) which are currently being promoted to the security industry are fit for the purpose of forming the signalling link from an intrusion and hold-up alarm system (I&HAS) to an alarm receiving centre (ARC).

The approach adopted in this guidance document is to evaluate, in terms of security, resilience and performance, the IP ATS products and services currently available or being trialled and, where necessary, relate the features of these to the 'traditional' signalling systems currently in widespread use. In other words, the observations and conclusions in the document are given within the context and framework of the services with which insurers are currently familiar and, essentially, comfortable. These 'traditional' systems operate on the premise that:

- activation of the alarm system elicits a police response at level 1;
- any fault preventing the correct operation of the alarm and/or signalling system at any time will be notified without delay to a keyholder (who, in most cases where alarm protection is an insurance requirement, will be required by policy terms to arrange for the premises to be attended until the fault is corrected).

This document contains a model (Appendix 1), to assist insurers and security providers to identify the features that, at the present time, the IPCRes committee considers to be the key indicators of a system acceptable for the protection of an insurance risk.

The model sets out the qualities and features that insurers would normally wish to see exhibited by an IP system. These are features insurers consider necessary for inclusion if the IP system is to be broadly comparable with 'traditional' signalling systems acceptable to insurers for all levels of risk. These include the most reliable and secure of the traditional systems currently available and that will continue to be installed for some time to come.

IP systems falling short of, or differing from, the model may well be acceptable to some insurers for certain risks, just as certain 'traditional' signalling systems are accepted on a selective basis despite the fact that there may be limitations in their performance.

The contents of this document should be read in the context of signalling connected to intrusion and hold-up alarm systems. Certain issues raised in the document are also relevant to IP signalling connected to other systems of great importance to insurers, such as CCTV or fire detection systems. While these issues are, for the most part, similar across the different types of systems, there are certain specific aspects which differ, so this guidance document should only be applied in the field for which it is intended.

2. Today's signalling scene

From the very earliest days of insurers' employment of intruder alarm systems for the protection of their risks, underwriters and surveyors have had a choice of signalling systems with differing performance. While there would be variation between competing insurers as to the risk level for which each type of system would be deemed to be acceptable, there would usually be a consensus in general terms as to the amount of confidence that could be placed in each method.

Currently, 'traditional' signalling products and services in widespread use are:

Single alarm transmission path

- Unmonitored public switched telephone network (PSTN) dial-up, ie digital communicator (low security).
- Monitored end-to-end telephone connection, eg BT redcare (high security).

Dual alarm transmission path

- Monitored packet switched radio primary path with unmonitored (including when in sole use) PSTN dial-up secondary path, eg CSL DualCom (medium security).
- Monitored packet switched radio primary path with monitored (including when in sole use) PSTN dial-up secondary path, eg CSL DualCom Plus (high security).
- Monitored end-to-end telephone connection primary path with monitored (including when in sole use) GSM (global system for mobile communications) secondary path, eg BT redcare GSM (high security).

A table giving an overview of the key features of the various signalling technologies currently in use is provided in Appendix 2.

Over recent decades, the security signalling market in the UK has addressed the varying needs for security, resilience and performance by adopting a variety of diverse signalling technologies. However, the signs are that this is unlikely to be the case in future as the telecommunications (or ‘telecoms’) industry in general adopts the internet protocol as the foundation for systems of all kinds.

3. The impact of IP

The latest transmission technologies are not designed around the traditional public telephone system or proprietary protocols. They employ ‘digitised’ data divided into discrete ‘packets’ transmitted over communications networks such as local area network (LAN), wide area network (WAN), WIFI, general packet radio service (GPRS), 3G, virtual private network (VPN) and/or the public internet.

Transmission control protocol/internet protocol (TCP/IP) and user datagram protocol/internet protocol (UDP/IP) are by far the most common internet protocols used to transport packet data (these protocols were explained in *Alarm signalling using the internet protocol: Part 1: An overview*). This network technology has found its way into most homes and businesses and the most common service is known as broadband or digital subscriber line (DSL). At the present time, most broadband circuits use the asynchronous digital subscriber line (ADSL) service – termed asynchronous because the data transfer rates of the upstream and downstream paths differ (the upstream path is slower).

Consumers are rapidly becoming aware of the advantages of digital solutions, such as fixed monthly costs, access to e-commerce, e-banking, voice over internet protocol (VoIP) telephony and many other online services. This communications revolution will shortly receive further impetus with the launch of BT’s ‘21st Century Network’ (21 CN), which involves the conversion of the core of the existing telephone system to one based on the internet protocol.

The security industry cannot ignore such fundamental changes to telecoms and commerce. In fact, it is beginning to appear that, when compared to IP systems, traditional signalling methods used in the UK security market may prove to be technically impracticable or uncompetitive at some point in the future.

The government has a digital strategy, the telecoms companies have digital strategies and commerce has long recognised the value of ‘being connected’. Now the security industry is having to develop its own strategies to ensure products and services are up-to-date and in line with mainstream technologies. Furthermore, more and more large companies are looking to reduce costs by applying fixed cost network solutions to security and other applications such as CCTV.

4. The impact on IP signalling of systems and equipment standards

British and European standards have an important impact on IP signalling – unfortunately through their inadequacy and lack of clarity rather than through the creation of a relevant and rational standards platform for the technology to be built on.

The most important documents containing references to signalling are:

- BS EN 50136: *Alarm systems. Alarm transmission systems and equipment* (various parts);
- BS EN 50131-1: 2006: *Alarm systems. Intrusion and hold-up systems. System requirements*;
- DD 243: 2004: *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice*;
- PD 6662: 2004: *Scheme for the application of European Standards for intruder and hold-up alarm systems*.

These standards were originally drawn up in the pre-IP era and, while they have been adequate for dial-up and direct line systems, they do not deal fully with new issues that arise with the use of IP. In fact, when read in an IP context, they can appear ambiguous.

There are a number of deficiencies and anomalies in the present standards when applied to IP systems. Probably the thorniest issue is the lack of clarity regarding what constitutes ‘alarm transmission equipment’ (ATE) and what constitutes ‘general network equipment’. According to BS EN 50136-1-1: 1998: *Alarm systems. Alarm transmission systems and equipment. General requirements for alarm transmission systems*, (clause 4.5), equipment such as a modem is classified as ATE if it is in use ‘**primarily** for the transmission of alarm messages’. This is an important issue, because if such equipment **is** classified as ATE, it must have power supply support and protection against tampering to the same level as control and indicating equipment (CIE). If it is **not** classified as ATE in terms of the standard, then it is viewed as general network equipment, in which case the standard is not contravened if transmission equipment such as an off-the-shelf modem/router is employed to connect to the network.

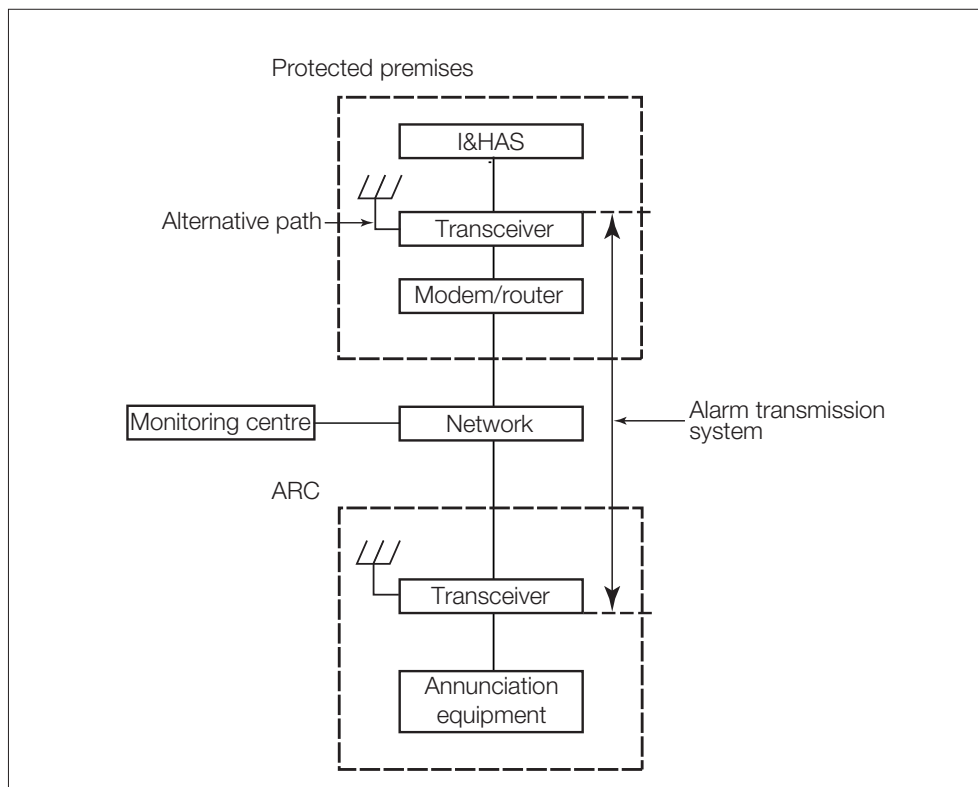


Figure 1: The essential elements of a typical IP alarm transmission system.

The question therefore arises: if the broadband service connected to the protected premises is used for both alarm messages and other traffic (eg business and/or recreational purposes), who is to say what the 'primary' use is? In the interests of the safety and security of the modem/router, insurers would tend to favour the provision of an additional broadband connection with a separate, protected and powered modem/router. However, promoters of the IP solution naturally point out that the provision of an additional broadband connection, with a separate, protected and powered modem/router, will make IP signalling much less financially attractive than it would otherwise be.

Another unhelpful feature of the standards is that it is not clear to the industry whether *multiple* ATs are synonymous with a *multiple path* AT. This leads to confusion and uncertainty. The standards identify classes of ATs that may be used in combination to achieve certain grades, but when it comes to establishing performance requirements in the event that one or other system develops a problem, the standards speak only of 'primary' and 'redundant' paths of an AT. This use of 'systems' and 'paths' creates confusion when applied to IP signalling system designs.

5. IP systems contrasted with other systems

In this section, specific facets of IP and traditional signalling methods are identified and contrasted.

5.1 ATs ownership and control

Responsibility for the system, or clearly defined elements of it, has until now not figured as an issue, as usually it has been clear where accountability lay. Traditionally it lay with the system supplier, installer, or maintainer, or a telephone or radio messaging system provider, or sometimes more than one of these simultaneously. However, if IP is being employed to connect to a remote site such as an ARC, the majority of systems will employ at least part of the public internet to complete the necessary path. Indeed, some proponents of IP signalling point out that businesses and householders will wish to recover their investment in 'always on' broadband services by also using the service for fire and security monitoring.

Hence the performance of the elements of the public internet conveying the signals will not be under the control of an identifiable or accountable party. If internet facilities are being provided by an internet service provider (ISP), it might be possible to identify aspects that are under the ISP's control, but this is not to say that an ISP could be held to account for how the services it is facilitating actually perform.

This introduces a degree of uncertainty as to whether actual performance and availability will indeed match the 'on paper' expectation. It is possible to bring evidence to show impressive speed of communication and high average availability using IP, but this does not alter the fact that in an individual case this might not be borne out by experience, eg due to the performance of the ISP selected by the user. In some large organisations, such as corporations or educational establishments, the telecoms network in use is largely under the organisation's control. However, the question then arises as to whether the security signalling path availability will be equal to that of an alternative proprietary signalling service. This may be something that management could find hard to absolutely guarantee to an insurer.

5.2 Responsibility for ATs troubleshooting

This is the issue that makes system control of such importance. Insurers and policyholders are accustomed to being able to identify the appropriate support point when the system falls into a fault condition. This will not always be the case with an IP system connected to the internet. The source of the problem and/or division of responsibility between the various parties – system supplier, installer, telecoms operator, ISP etc – might be extremely challenging for the average user to pin down quickly. In the absence of a support service it may be far from clear to a non-technical user how to ensure that a problem is corrected and the security of the premises reinstated within the necessary timescale.

However, if the system is designed carefully, it is possible to recognise whether a failure has occurred in:

1. the local loop (the copper/fibre connection to the local telephone exchange);
2. the network (including, if applicable, the internet); or
3. the 'last leg' – the connection (or one of the connections) to the ARC from the ARC's local exchange.

It is therefore prudent to select only those carefully designed IP ATSS that are engineered to allow at least this depth of fault analysis. It is also wise to ensure that IP ATSS are only terminated at ARCs that undertake, contractually, to offer troubleshooting of all ATS faults, and function as a single point of contact for ATS problems of any and all kinds.

Are transmission systems using the internet protocol all the same?

No, there are differences in approach among the designers of systems. At the time of publication, there are essentially two basic service configurations on the market:

1. **Point-to-point service.** The intruder alarm system sends signals to the ARC using the IP signalling supplier's proprietary equipment at both ends. The ARC has primary responsibility for monitoring whether the signalling link is operating correctly. The ARC usually receives technical and analytical support from the IP signalling supplier.

However, the actual extent and limitations of the support available to the alarm system owner need to be established at the outset with the ARC, as these might vary between the ARCs that offer a service based on the signalling supplier's products.

2. **Monitoring centre based service.** The signals from the alarm system pass through a monitoring centre operated by the IP signalling supplier en route to the ARC. In effect, the monitoring centre is at the hub of a network, the outstations of which consist of ARCs that have elected to monitor the supplier's signals.

Unlike the point-to-point type of service, a monitoring centre based service has the potential to offer a single point of contact (ie the monitoring centre) for troubleshooting and accountability for the availability and performance of the IP signalling system in its entirety.

5.3 How suitable is the internet for security signalling?

Is the internet sufficiently secure for alarm signalling? Vital telecoms security measures, such as authentication and message integrity verification, should always be designed on the assumption that skilled and determined criminals will be able to gain unauthorised access to the signals for the purpose of manipulating them. Accordingly, the best practice defences in the relevant document (BS EN 50131-1), ie those for substitution security and information security, are as relevant to an 'open' system (such as the internet) as they are to a 'closed' system such as a private line or network.

Nevertheless, there is a natural anxiety among specifiers accustomed to traditional 'closed' proprietary systems that the 'open' public internet is a magnet for, and intrinsically insecure against, a range of potential 'hackers' bent on theft or disruption of one form or another. In fairness, this fear is not always entirely rational and can be overdone. However, the fact remains that the technology has a tarnished track record from notorious 'exploits' in the past, some of the most publicised of which involved mass traffic flooding such as distributed denial of service (DoS) attacks on household name organisations, such as on-line retailers. Therefore, the credibility of IP/the internet does hinge on the industry staying one jump ahead of electronically-minded criminals.

Proponents of IP point to the fact that networks using the internet protocol are used for secure transactions by financial institutions. Others, however, point out that financial networks are specifically designed for that application and that to set them alongside

security alarm signalling is not comparing like with like. Once again we come up against the fact that the requirements of existing standards are limited in the security area because they were not drawn up with IP signalling via the internet in view. They do not, for example, deal with attacks which are characteristically carried out against IP/internet systems, such as viruses or denial of service attacks – albeit that well-designed IP equipment should have limited exposure to such attacks compared with, say, a personal computer (PC). Indeed some proponents of IP security signalling assume that the firewall arrangements at the protected premises can be left as the responsibility of the user inasmuch as the user's own, regular, off-the-shelf broadband router will be employed. Firewalls built into mass market routers, in combination with the firewall properties of current operating systems like Windows XP, are considered by industry experts to be adequate for low-level risks. However, for risks that would demand a high level of security, the fact that there is no industry standard or convention for the specification of a firewall where an alarm system is connected must be a concern for insurers.

Existing traditional signalling systems are not without security vulnerabilities, but their weaknesses are understood, insurers have the measure of them and are able to factor them into their risk assessment. This cannot yet be said for IP signalling via the internet without more experience of it.

Reliability should also be considered when assessing the suitability of the internet for signalling. As inferred above, the dependability of the system might be greatly impacted by the actions of the user's chosen ISP, which has no particular accountability to ensure that security alarm signals get through. ISPs and network operators in an intensely competitive market must ensure that margins are protected and this has resulted in practices in their industry that arguably place the signalling at risk and have no equivalent in traditional systems. Some examples that illustrate this follow:

- 'Contention'

All customers sharing a broadband channel connected to the internet are in contention with others for the available capacity. 'Contention' in this context means that the available bandwidth is shared by a number of users. This is usually denoted by a ratio, so on a 50:1 system, 50 users compete for the same bandwidth. A high contention ratio and/or heavy usage by other sharing users will detrimentally affect speed and service during periods of heavy shared usage. Providers have to make a calculation based on the number and type of users and the available capacity. Other than the normal action of the marketplace, there does not appear to be any formal regulatory arrangement, industry-policed or otherwise, to constrain the providers. The IP signalling manufacturers and independent authorities are comfortable that contention will not materially affect the transmission of intrusion and hold-up alarm signals, as the data block being transmitted is comparatively tiny (and a place for it in the 'queue' is found after only a very short delay). However, contention might well have an impact when other security data that is more 'bandwidth hungry' (such as supporting CCTV images) are required to be transmitted.

- Broadband 'fair usage' policy

Most ISPs apply a 'fair usage' policy to broadband services. This typically takes the form of a monthly limit on the amount of data that can be sent/received from a site. Once this limit is exceeded, the ISP can restrict the bandwidth and in some cases ISPs suspend the service altogether for the remainder of the month. Such restrictions and the contention ratio vary both by ISP and the individual service package. Broadband services with unlimited usage and realistic contention ratios (usually business packages) should be selected. Selection of the ISP and responsibility for ensuring that the services remain suitable for alarm transmission purposes are, of course, in the domain of the user/policyholder, who will be sensitive to charges but may not be aware of the implications for service and performance.

- Broadband planned outages

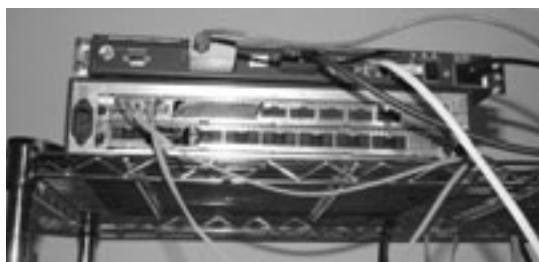
From time to time, ISPs notify users of planned outages necessary for maintenance and upgrades. ISPs such as BT often post maintenance notices on their websites, especially if the DSL system will be interrupted for long periods. This information could be used by criminals with inside knowledge. How is a user/policyholder to know that this practice might not be introduced, even if assurances are received on day one? Is planned outage information available other than as public announcements, eg within the information technology (IT) industry? This is an issue that arguably has an impact on telecoms infrastructures in general (not just IP) as the industry moves from traditional methods to large-scale, shared, and electronically-managed networks.

5.4 ATS components

Reference was made earlier to the fact that there are critical components that some IP ATE/ATS suppliers are assuming may be left to the user to supply and maintain. In a single premises application such as a dwelling or a small- to medium-sized business, these components include the DSL modem, firewall, router, and hub etc. These broadband system elements may be assembled together in one unit, often termed 'the router' or 'modem/router', or kept separate and connected by plug-in cabling. This creates an issue that does not exist in the same way with proprietary traditional signalling systems, namely that the unit or units concerned are exposed to having their connections and mains power supply interfered with, innocently or malevolently. Should they be disconnected, an ATS fault will be registered within a short time (ie as per the grade of ATS required by the model provided in Appendix 1 of this guidance document). However, in many environments this exposure will, at the very least, cause the credibility of the alarm system to be put in jeopardy and at worst, might lead to reduced protection or spurious confirmed alarm conditions.

Good practice dictates that 'the router' has the same security and power provision as the alarm CIE. The existing standards may be unclear on whether this is actually a requirement, but opinion among insurers is that if a comparison on this issue is to be made with traditional signalling, 'the router' needs to be within a secure, tamper-protected cabinet, with power provision to the same standard as the CIE. However, if the DSL service must be available for other purposes (recreational and/or business) the customer may require that 'the router' be readily accessible. For this reason, it may be unavoidable in some cases that an entirely separate DSL service is connected to the premises for alarm signalling.

The IP ATS may be designed to operate through the customer's own modem/router rather than a modem/router supplied as part of the alarm transmission equipment and supported by a source of stand-by power and anti-tamper protection.



5.5 ATS availability

The European systems standard BS EN 50131-1 no longer contains requirements for availability as part of the criteria for each grade of ATS. However, the model provided in Appendix 1 of this guidance document recommends that the minimum ATS grade that insurers should accept is ATS grade 5 with an availability of class A4 according to Table 4 of BS EN 50136-1-1, paragraph 6.4.5. This equates to 99.8% availability (or 17 hours non-availability) in any 12-month period.

A crucial issue, however, is the fact that the providers of the backbone of the ATS (ie normally a broadband DSL service), such as BT and other networks licensed to provide telecoms services in the UK, do not usually offer quality of service (QoS) information or service level agreements (SLAs). If a policyholder wishes to use an

ISP to link the alarm system to the ARC, it may be possible to obtain QoS information (such as connection availability) from the ISP, or, better still, from an independent third party. In the absence of such information, the confidence that the insurer can have in the IP signalling solution must be diminished to one degree or another. However, responsible players in the IP signalling marketplace, recognising the key significance of availability for all aspects of IP signalling performance, are making strenuous efforts to evaluate availability factors and establish industry-wide systems for monitoring and maintaining suitable availability levels.

5.6 Polling

In order to verify the continuity of protection there must be a mechanism by which the availability of the alarm transmission path between the protected premises and the ARC can be checked or 'polled'. This takes the form of data exchange from the monitored site to the ARC (or vice versa) via the IP system's communication network. In all cases the polling must occur within a given timescale for the relevant grade so that a fault will be reported within the minimum reporting time set for the grade in BS EN 50136-1-1. Where dual path signalling is used, the system should continue to poll over the secondary route if the primary route fails (however, some ATE/ATS providers claim that the standard is ambiguous as to whether the secondary path is required to report faults to the same standard as the primary path when the primary path is in fault and the secondary path is in use for transmission).

One reason why the model provided in Appendix 1 of this guidance document identifies the signalling performance criteria of ATS 5 as the minimum for insurance-specified systems is that these criteria require reporting class T4 (maximum 180 seconds). This is considered a prudent minimum monitoring frequency for an intruder alarm system meeting system grade 3 (according to BS EN 50131-1), and is also the reporting interval favoured by many insurers for the majority of commercial risks requiring police response. If insurers relied on the minimum signalling criteria available to installers at system grade 3, without invoking the IPCRes model (or nominating an ATS by brand name), it would be perfectly legitimate for an installer to supply an ATS reporting no more frequently than every five hours, an interval considered unacceptable to most insurers in the UK.

Some IP ATS equipment is manufactured with a variable poll period that is intended to be set during installation/commissioning. Typically, the poll period is set for the particular class of system by the ARC. It is vital, therefore, that there is an assurance that this poll period will not be altered from the specified setting without the written permission of the owner of the I&HAS.

5.7 Use of 'in-house' networks

Many companies have existing computer networks linking their sites, and management may be persuaded of the economic benefits of using their in-house IP network for fire and security signalling.

However, this might represent a dilemma for an insurer, as the performance of the signalling could be at the mercy of those in the firm with control over the configuration/operating parameters of the network. For example, it may be possible for the network technicians to suspend the connection from a given location for engineering reasons and the fact that this has occurred, and/or its consequences, may not be known to management.

Depending on the circumstances, insurers may prefer that IP alarm system signals do not employ the company infrastructure, but that a separate and independent IP system is used, with a dedicated DSL circuit.

5.8 Positive features of IP signalling

There are many points of difference between traditional signalling methods and IP signalling but these are by no means all negative by nature. A counterbalance to many of the uncertainties identified in this guide is that a fundamental, structural quality of IP networks, and the internet itself, is that messages comprise numerous

discrete ‘packets’. Each packet is an individually addressed element, capable of being channelled to its destination by any one of a number of different routes. This endows networks with a ‘self-repairing’ quality – packets that fail to arrive via one route are redirected to their destination via another. In addition, the technology allows messages to be sent to multiple destinations without any need for the additional fixed channels that would be necessary using traditional telecoms technology. Furthermore, the pricing structures for internet and GPRS services are such that, unlike previous systems, network charges are not a significant obstacle to polling at the most frequent rates. A further advantage is the great speed with which signals are processed, which allows recovery of undelivered data packets within timeframes such that the quality of service is, for all practical purposes, unaffected.

6. Summary

New IP signalling products and services are coming onto the market and, to one degree or another, they vary in how they function. In the absence of a standard or market convention for the design of systems, insurers have no choice but to investigate and assess the relative strengths and the special features of each, and to match the competing systems to the types of risk they underwrite. As the technology in this application is in its infancy, there may be no choice but to accept certain claims about the technology at face value and evaluate the impact on levels of service and security over time. With the rapid rate of change that tends to be a feature of telecoms services, there are likely to be a number of different approaches in the pipeline.

For ease of reference the following table summarises the key issues raised in this report, together with comments and recommendations. The key issues are classified under the three broad headings of security, resilience and performance.

Table 1: Summary of key issues

Topic	Comment	Recommendation
SECURITY		
Information substitution	It is vital that alarm information cannot be intercepted and changed en route to the ARC	An ATS should meet the substitution requirements of ATS 5 as per BS EN 50131-1
Information encryption	It is vital that alarm information cannot be read en route to the ARC	An ATS should meet the encryption requirements of ATS 5 as per BS EN 50131-1
Denial of service (DoS)	While a DoS or hacking attack via insecure password protocols may be possible against some parts of shared-use IP networks, alarm systems are not normally vulnerable to direct external interference as they do not use normal computer programmes	In order to reduce this type of threat, an IP system using dedicated equipment should be employed. If the IP system does not use dedicated equipment, there should at least be frequent polling to alert alarm owners/users to any problem
Planned downtime	Some IP networks/ISPs publish planned downtime, with the risk that professional criminals may choose such times to execute a break-in. IP networks dedicated to alarm traffic are unlikely to advertise downtime	A second signalling route should ideally be provided to enable alarm signals to be sent during any such downtime period
Shared equipment	Only one DSL modem can be fitted to a broadband line, so if the potential cost savings of IP signalling are required, ie broadband is fitted/used for other purposes, it will usually be necessary for the ATS to share network equipment	In effect, selection of level A of the IPCRes model in Appendix 1 leads to the use of a dedicated DSL and is therefore the recommended choice. At the very least, it should be ensured that level B is achieved. In either event, there should be frequent polling to alert alarm owners/users to any problem

Table 1 continued

Topic	Comment	Recommendation
RESILIENCE		
Tampering	It is important that any tampering with ATS equipment is detected, which might not be possible where the ATS utilises a shared-use network and equipment	ATS equipment should preferably be installed to meet level A of the IPCRes model, but otherwise should be sited in an area with adequate intruder alarm detection, meeting level B of the IPCRes model
Power supplies	Failure of mains power will mean that an IP ATS will be unable to operate. While mains power loss may be detectable and notified to the ARC, if there is no battery back-up, an insurer will usually require a keyholder to attend the premises until the network is restored	ATS equipment should preferably be installed to meet Level A of the IPCRes model, but otherwise, frequent polling will at least alert alarm owners/users to any problem
Equipment connections	Unless all IP ATS equipment is hardwired and mechanically connected, (which might not be possible where the ATS utilises a shared-use network and equipment), users, visitors or criminals may accidentally or deliberately disconnect the signalling	In order that users are made aware of faults as they try to set the alarm system, all signalling paths must be monitored locally (as per PD 6662). When the alarm is set, frequent polling will at least alert alarm owners/users to any problem
PERFORMANCE		
Fault reporting time	An alarm signalling system should be frequently checked to ensure that it remains available and operational. Inexpensive IP polling makes a 3-minute fault reporting interval financially viable on the primary path and, when in sole use, any secondary path	An ATS should meet the reporting time requirements of ATS 5 as per BS EN 50131-1, and, when any secondary path is in sole use, the stepped-up reporting times of the IPCRes model
Contention	Where alarm signalling is competing for available space, especially if shared networks/equipment are used, there is a possibility that signals could be delayed or not sent. IP networks dedicated to alarm traffic are less likely to suffer. However, given the small size of data packets/high re-transmission speeds, signals carried on shared networks and/or the public internet are likely to get through with tolerable delay despite contention with other services	As a safeguard against the potentially adverse effects of contention (and other threats to a signalling system based on IP), the model in Appendix 1 contains a recommendation for availability reporting
Availability	The more unreliable an IP network is, the more often an alarm using it will cease to be fully operational. In circumstances of network failure, an insurer will usually require a keyholder to attend the premises until the network is restored	While existing standards do not require a particular level of availability to be met, it is desirable that high figures are achieved, ie as per BS EN 50136-1. Therefore, the availability levels of a given network should be established before the alarm signalling is connected and, following connection, should be subject to continuous monitoring, especially if shared networks/equipment are used
Network repairs	If a network/signalling path fails it needs to be restored. The more people there are involved in maintaining a network, the more potential there is for confusion and delay in making repairs, and the longer the time a keyholder may need to remain at the premises	Responsibility for repairs should be taken by one body, eg an ARC or signalling network provider, with a single point of contact for alarm owners/users available '24/7'

7. Conclusion

There are undoubtedly benefits associated with IP signalling, many of which surround cost and competition in the signalling marketplace – a sector which is expected to expand in the near/middle term. There will be the incidental benefit for the insurance and security industries alike in that policyholders in general, who by the day grow more familiar and comfortable with the internet, will see the benefits of having their unmonitored security systems enhanced by the provision of monitored remote signalling.

However, as this guidance document sets out, there are some potential security and resilience issues surrounding IP signalling at the present time. The degree to which these will prove significant to insurers may not be known for a while. Meanwhile, faced with pressure from valued customers to entertain risks protected by IP signalling systems, it is anticipated that insurers will progressively adopt IP on a tentative basis, at least in the immediate future, although some may not be prepared to accept its use on their larger security exposures.

There is intense debate in the security and insurance industries as to how IP ATSS should be designed and operate. Until cogent regulation is in place, any template or model such as the example in Appendix 1 of this document will inevitably prove to be contentious. Having studied this subject for a considerable time, IPCRes has had to conclude, reluctantly, that in the present environment, it is not going to be possible to provide insurers with a mechanism whereby a given IP ATS can be assessed for suitability in a way that can be implemented every day by non-technical staff. It is hoped that the IPCRes model will influence system providers to adopt good practice in the design of new systems, and increase the prospect of ready acceptance by insurers.

Claims of compliance with the model could serve as a method of discriminating between the various designs making their appearance. Some insurers may be able to apply the model in assessing individual systems and establishing their own in-house criteria for approval. However, IPCRes does recognise that the model is not a completely satisfactory mechanism and it is seen as an interim measure while standards are established and approval schemes based on them are developed. These should follow in the medium term.

Meanwhile, in the interests of creating a 'level playing field' in the signalling marketplace, insurers feel that it would assist the security industry, specifiers and users if any interpretations of present standards made by regulatory bodies or expert groups are promulgated formally and placed in the public domain. IPCRes also urges accredited test houses and approvals bodies to accelerate progress towards implementation of approval schemes tailored to IP signalling technology. Such schemes might grade ATS types (preferably taking account of the suggested criteria in this document's model). Subject to such schemes embodying a requirement for ongoing product sampling and factory production control, insurers will have practical means to match systems to insured risks and should feel encouraged to support and promote IP technology to the benefit of system suppliers.

Appendix 1

Insurers' model for IP-based alarm signalling systems

This document models insurers' likely expectations of IP-based alarm transmission systems (ATSs) that can be deemed to provide secure and dependable alarm signalling from an intrusion and hold-up alarm system (I&HAS) at an alarm-protected premises to an alarm receiving centre (ARC).

It applies to all IP-based dual path ATSs, as might typically be installed with new or existing confirmation alarm systems, and, in limited circumstances, to single path ATSs that may be encountered, for example, with some non-confirmation alarm systems.

1. Subject to meeting the design and performance criteria in paragraphs 2 to 8 below, insurer acceptance of dual or single path IP-based ATSs is likely to be as follows:

Dual path systems – Acceptable with all alarm system types.

Single path systems – Acceptable where a non-confirmation alarm system with an unmonitored signalling service, eg a digital communicator, is being upgraded to provide monitored signalling.

2. According to the nature of alarm signalling required, alarm signals should be sent to the ARC as follows:

Dual path systems

- (i) by an ATS that meets or exceeds performance criteria ATS 5* and has two alarm transmission paths, each utilising different technologies – ie a 'dual path' system as per DD 243: 2004: *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice*;

Or:

- (ii) by two ATSs, one meeting or exceeding performance criteria ATS 5* and the other meeting or exceeding performance criteria ATS 4*, each ATS utilising different technologies – ie a 'dual path' system as per DD 243.

Note: Should one alarm transmission path or ATS cease to function in accordance with its performance criteria, the remaining alarm transmission path or ATS should meet, or exceed, the reporting time class T4* throughout the period during which it is the only alarm transmission path or system available.

Single path systems

- (i) by an ATS that meets or exceeds performance criteria ATS 5*.

3. One of the following levels of provision shall be made to guard against the risk of power failure, accidental or deliberate disconnection or interference with any signalling equipment through which signals pass before leaving the protected premises (for the purposes of this document, 'signalling equipment' includes the transceiver, ATE/ATS hub, firewall, DSL modem, router and similar equipment):

Dual path systems

Either: Level A

All 'signalling equipment' used in relation to each alarm transmission path:

- (i) shares a common power supply with that of the alarm CIE, or has equivalent provision in terms of loss reporting and battery back-up to that required by the BS/EN standards applicable to the particular alarm system; and
- (ii) is located inside the CIE cabinet, or has equivalent provision in terms of both tamper protection, detection and reporting, and fault detection and reporting, to that required by the BS/EN standards applicable to the particular alarm system.

*as defined in BS EN 50131-1: 2006: *Alarm systems. Intrusion and hold-up systems. System requirements*.

Or: Level B

All 'signalling equipment' used in relation to one of the alarm transmission paths meets the requirements of level A (above), while all 'signalling equipment' used by the other path is located in an area(s) where entry will immediately generate a full alarm activation (while the alarm is fully set). Specifically, the signalling equipment is **not** sited in an area configured as an alarm 'entry route' and, for a confirmation alarm system, **is** sited in an area where a confirmed activation can be generated.

Single path systems

All 'signalling equipment' should be installed in accordance with level A above.

4. A detectable fault on any ATS or alarm transmission path should be indicated to users at the time of setting and logged by the CIE.
5. The fault 'reporting time' of the ATS should be set at the time of installation or commissioning to meet the requirements of point 2 of this model and should be recorded in the alarm specification or 'as fitted' document. No subsequent alteration of 'reporting time' parameters should be made without the written agreement of the I&HAS owner/user.
6. Providers of IP-based ATSS should provide information on compliance with network 'availability', as per class A4 of Table 4 of BS EN 50136-1-1, paragraph 6.4.5.
7. Where use is made of an internal IP network shared with other services, checks on the likely compliance with (6) above should be made.

Note: where poor availability is indicated or such figures are not available, it is recommended that a dedicated DSL be used instead.

8. Clear written information should be provided to the owner/user of an I&HAS as to where accountability and responsibility lie for the performance, maintenance, repair and management of specific parts of, or the entire, ATS.

Note: IPCRes considers adherence to this model necessary to ensure insurers have confidence that IP ATSS are comparable in terms of security and performance with 'traditional' signalling systems. However, insurers need the flexibility to appraise security on an individual risk basis and different configurations from those outlined above may be required in certain circumstances.

Appendix 2

Table 2: Overview and comparison of the key features of the principal types of technology and media currently used for fire and intruder alarm signalling.

	Method	Strengths	Limitations
PSTN dialler	Dials ARC and sends coded message	<ul style="list-style-type: none"> - simple, reliable 	<ul style="list-style-type: none"> - risk of interference with physical line (high risk) - amount of data transmitted is limited - slow - cannot be securely monitored by ARC
Carrier signal via telephone line (ie BT 'redcare')	Employs telephone connection to carry superimposed in-band and out-of-band (ie audible and inaudible) signals, which are processed at the local exchange and relayed onto the ARC via a proprietary network	<ul style="list-style-type: none"> - securely monitored - fast - tailored network dedicated to alarm signalling market with own fault monitoring/control 	<ul style="list-style-type: none"> - risk of interference with physical line (limited risk) - amount of data transmitted is limited - available only on BT telephone services
Packet switched radio	Signals to network of base stations and on to ARC via network control centre	<ul style="list-style-type: none"> - securely monitored - fast 	<ul style="list-style-type: none"> - proprietary network selected may have less diverse routing than GSM/GPRS - amount of data transmitted is limited - signal strength fluctuation may be an issue - alarm users contend with non-alarm users on network - skilled installation essential
GSM	Employs the GSM short messaging service (SMS) of one of the cellular radio provider's networks	<ul style="list-style-type: none"> - securely monitored - fast - capable of carrying a limited amount of event information - no physical line to be concerned about 	<ul style="list-style-type: none"> - possible signal strength fluctuation and/or interference - may be contention between alarm users and non-alarm users - exposed to risk of jamming - skilled installation essential
IP via GPRS	Employs the GPRS service of one of the cellular radio provider's networks	<ul style="list-style-type: none"> - securely monitored - fast - capable of carrying a generous amount of event information - no physical line to be concerned about 	<ul style="list-style-type: none"> - possible signal strength fluctuation and/or interference - may be contention between alarm users and non-alarm users - exposed to risk of jamming - skilled installation essential
IP via telephone line	Employs telephone connection to carry a superimposed out-of-band DSL circuit conveying IP-based event and other data	<ul style="list-style-type: none"> - securely monitored - fast - capable of carrying a generous amount of event information - medium may be shared with recreational/business uses without degrading alarm function 	<ul style="list-style-type: none"> - risk of interference with physical line (limited risk) - ISP network may provide limited and/or undependable QoS information - in-house QoS subject to variation - key components in protected premises are exposed to interference unless safeguards are implemented by the system provider - exposure to denial of service attack

Abbreviations/Glossary

This glossary contains explanations of terms used in this document, plus others that are commonly used in connection with telecoms in general and ATSS in particular.

3G

3G refers to the 'third generation' of developments in wireless technology, especially mobile communications. 3G is a service using a higher bandwidth (see below) than earlier generations of the technology and providing advanced capabilities and features, such as enhanced multimedia (voice, data, video, and remote control) and roaming capability throughout Europe, Japan, and North America.

802.11

A group of specifications for wireless networks developed by the Institute of Electrical and Electronics Engineers (IEEE). 802.11 uses the ethernet protocol (defined below) and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.

ADSL: Asynchronous (or asymmetric) digital subscriber line

A technology for transmitting digital information at high bandwidths on existing phone lines. Unlike regular dial-up phone services, DSL technology provides a continuously available connection. ADSL is asynchronous (asymmetric) in that it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. ADSL simultaneously accommodates analogue (voice) information and digital information on the same line.

Annunciation equipment

Equipment located at an alarm receiving centre which displays the alarm status, or the changed alarm status, of alarm systems, in response to the receipt of incoming alarm messages (definition from BS EN 50136-1-1).

ARC: Alarm receiving centre

A continuously manned centre to which information concerning the status of one or more alarm systems is reported (definition from BS EN 50136).

ATE: Alarm transmission equipment

Equipment which is used primarily for the transmission of alarm messages from the supervised premises transceiver interface to the alarm system interface, to the receiving centre transceiver interface, to the annunciation equipment (definition from BS EN 50136).

ATS: Alarm transmission system

Equipment and network used to transfer information concerned with the state of one or more alarm systems to one or more alarm receiving centres (definition from BS EN 50136).

Bandwidth

A measure of the capacity of data that can be moved between two points in a given period of time. Most network managers consider 50% bandwidth usage to be the maximum data throughput. Any higher data throughput usually requires more bandwidth.

CIE: Control and indicating equipment

Control and indicating equipment of the I&HAS (see below).

Contention

Competition by users of a network for access/use at the same time. The term 'contention ratio' applies specifically to the number of people connected to an ISP who share a set amount of bandwidth. Example values would be 50:1 for home users (that is to say that 50 people or lines will vie for the same bandwidth) and 20:1 for business users.

DoS: Denial of service

A type of attack on a network designed to sabotage it by flooding it with spurious traffic. There are damage-limiting software fixes to guard against some, but not all, types of attack. DDOS (distributed denial of service) attacks, while unlikely in the context of alarm system signalling, have the potential to cripple a targeted computer.

DSL: Digital subscriber line

A technology for transmitting digital information at high bandwidths on existing phone lines. Unlike regular dial-up phone services, DSL technology provides a continuously available connection. The DSL service may be asynchronous (ADSL) or synchronous (SDSL).

Ethernet

A computer network cabling system designed by Xerox in the late 1970s. Originally transmission rates were 3 megabits per second over thick coaxial cable. Media today include fibre, twisted-pair (copper), and several coaxial cable types. Rates are up to 10 gigabits per second or 10,000 megabits per second.

GPRS: General packet radio service

A standard for wireless communications which runs at speeds of up to 115 kilobits per second, compared with current GSM (global system for mobile communications – see below) systems' 9.6 kilobits per second. GPRS supports a wide range of bandwidths. It is an efficient use of limited bandwidth and is particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing.

GSM: Global system for mobile communications

Originally developed as a pan-European standard for digital mobile telephony, GSM has become the world's most widely used mobile system.

I&HAS: Intrusion and hold-up alarm system

An intrusion and hold-up alarm system (I&HAS) is a combined intruder and hold-up alarm system. An intruder alarm system is an alarm system to detect and indicate the presence, entry or attempted entry of an intruder into supervised premises. A hold-up alarm system is an alarm system providing the means for a user to deliberately generate a hold-up alarm condition (taken from definitions in BS EN 50131-1).

IP: Internet protocol

The internet protocol is a method, or protocol, by which information can be sent from one computer to another on a network. The data is divided into numerous 'packets' (see below), within which the data is assembled in a format or pattern that takes a consistent form. However, the IP is responsible only for the configuration of the packet – other protocols, such as TCP (see below), are required for effective communication. Nevertheless, in the context of a guide such as this, the term 'IP' is used as convenient shorthand to label the use of 'IP technology' for a specific application – in this case alarm system signalling.

ISDN: Integrated switched digital network

Digital network with higher speed than found on the traditional telephone network. Even though ISDN uses existing phone lines, it does require specialised equipment. Because the network is all digital it can easily send voice, data, and video over the same line simultaneously.

ISP: Internet service provider

An ISP provides access to the internet for others via connectivity service(s). This might be in the form of dial-up services, DSL, web hosting services or a combination of these.

LAN: Local area network

A local area network (LAN) is a computer network covering a local area, like a home, office or small group of buildings, such as a college.

Modem

A modem modulates outgoing digital signals from a computer or other digital device to signals that are suitable for being conveyed on conventional (copper) telephone line and demodulates the incoming signal, converting it to a digital signal for the digital device.

Monitoring centre

A manned remote centre in which the status of one or more alarm transmission systems is monitored (definition from BS EN 50136-1-1).

Packet

A packet is a formatted block of 'digitised' data conveyed by a computer or telecoms network. The contents of an IP packet are arranged according to the conventions of the internet protocol. Packet communication contrasts with communications links that do not support packets, such as traditional point-to-point links that simply transmit data in a serial stream. When data is formatted into packets, networks can transmit longer messages more efficiently and reliably.

Packet switched radio signalling

A packet communication system (see above) employed in proprietary ATs that use radio as the communication medium (as opposed to physical links such as telephone lines).

POTS: Plain old telephone system

Conventional analogue telephone service.

PSTN: Public switched telephone network

Also known as plain old telephone system (POTS), this refers to the world's collection of interconnected public telephone networks designed primarily for voice traffic.

QoS: Quality of service

Generally taken to mean transmission rates, error rates and other characteristics that can be measured, improved and, to some extent, guaranteed in advance.

redcare

An alarm transmission service operated by BT, offering a secure method of transmitting signals from an intruder alarm panel to an ARC.

Router

The router is the device that determines the next network point to which an IP 'packet' (message) is to be forwarded towards its destination. However, use of the term in the context of the home or small business user is generally taken as referring to a product that actually consists of the router plus the internet modem and an on-board firewall.

SDSL: Synchronous (or symmetric) digital subscriber line

A technology for transmitting digital information at high bandwidths on existing phone lines. Unlike regular dial-up phone services, DSL technology (see above) provides a continuously available connection. SDSL is termed 'synchronous' (or 'symmetric') because it supports the same data rates for upstream and downstream traffic. A similar technology that supports different data rates for upstream and downstream data is termed ADSL (asynchronous digital subscriber line).

SLA: Service level agreement

A contractual agreement between, for example, an ISP or an ATs provider and the service user, setting out the parameters that the services being provided will be maintained within.

SMS: Short messaging service

Available on digital GSM networks, SMS allows text messages of up to 160 characters to be sent and received via the network operator's message centre to or from a mobile phone, or to or from the internet, using a so-called 'SMS gateway' website. If the phone is powered off or out of range, messages are stored in the network and are delivered at the next opportunity.

TCP/IP: Transmission control protocol/internet protocol

A protocol for communication between computers, used as a standard method for transmitting data over networks and as the basis for standard internet protocols.

Transceiver

A communications device capable of both transmitting and receiving.

UDP/IP: User datagram protocol/internet protocol

UDP/IP is one of the core protocols of the IP suite of protocols. Using UDP/IP, programs on networked computers can send short messages (sometimes known as datagrams) to one another. UDP/IP does not provide the reliability and ordering guarantees that TCP/IP does. However, UDP/IP is faster and more efficient than TCP/IP for small data packets such as alarm signals.

VoIP: Voice over internet protocol

The technology used to transmit voice conversations over a data network using the internet protocol. The data network may be the internet or a corporate intranet.

VPN: Virtual private network

A VPN is a private communications network, often used within a company, or by several companies or organisations. A VPN 'segregates' a section of an existing larger network (which may be accessible to others, such as the public internet), and, by restricting access, allows the communications traffic to remain confidential. While the communications protocols in use are essentially those of any IP-based network, special measures are built into a VPN to try to ensure that access to the VPN is restricted to the computers of the legitimate VPN users.

WAN: Wide area network

A wide area network or WAN is a computer network covering a wide geographical area, involving a vast array of computers. The best example of a WAN is the internet.

WiFi

WiFi is a branded technology for wireless local area networks (WLAN), based on the IEEE 802.11 specifications. It was developed to be used for mobile computing devices, such as laptops in LANs, but is now increasingly used for more services, including internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras.

Other IPCRes guidance documents

Other documents developed under the Insurers' Property Crime Research (IPCRes) scheme include:

Intruder alarms and a harmonised European standard

This guidance document reviews the progress that has been made in pursuit of a harmonised European Standard for the design and installation of intruder alarms and offers practical advice for those uncertain about their choice of intruder alarm.

Alarm signalling using the internet protocol: Part 1: An overview

This document is aimed at those seeking an introductory understanding of different methods of transmitting security alarm data over local area network and wide area network infrastructures, using internet-based protocols.

It investigates and reports on internet protocol (IP) signalling designed to be used to transmit intruder, hold-up and other critical signals from a monitored location to an alarm receiving centre.

Convenience ATMs: Recommended security measures

This document provides advice on the security of 'stand-alone' or 'freestanding' automated teller machines (ATMs), typically located in convenience stores, petrol stations, supermarkets, pubs, and clubs etc. The guidance given within this document is designed to reduce the risk of crime and therefore insurance losses occurring on premises where such ATMs are installed.

Electronic security systems: Guidance on keyholder selection and duties

The purpose of this guide is to assist owners of electronic security systems at commercial premises in selecting appropriate persons to act as premises keyholders. It also provides guidance on ensuring the safety of keyholders, and keyholders' responsibilities when operating the system or attending the site in response to an activation/fault.

Security fog devices

These guidelines have been produced to assist potential users and specifiers in understanding certain factors that need to be considered before installing a security fog device.



IPCRes **guidance**

InFiReS
Insurers' Fire Research Strategy funding scheme

Alarm signalling using the internet protocol Part 2: Considerations for insurers

