

The Risks and Rewards of IP Signalling

In this article Jim Winter, Ascom Security Communications UK, gives an overview of the issues surrounding the use of IP in security systems, including:

- Why installers and clients should get ready to change to IP.
- The things installers need to know to make sure they can set up IP systems quickly and efficiently to meet the needs of regulators (SSAIB).

IP stands for 'Internet Protocol', which is a sophisticated method of transmitting data from one place to another via the Internet. When it's done well, IP is the ideal way to transmit alarms, because it's:

- Secure
- Very fast
- Easy to use
- Cost effective – moving to IP instead of continuing to use outdated systems will cut most customers' bills by a third or even half over three years and that is quite a saving!

Since it was first introduced, there has been some debate about whether IP is the best choice for alarm transmission needs. As with any advance in technology, there were those who approached this new idea with apprehension and concern. The majority of people in the industry have now been won over though, as IP has proved itself to be so reliable, simple to use, and cost effective. Essentially, the market has realised that yes, it is that good, and moved on.

Supporting technology has moved on as well. Nowadays, you can get a strong broadband internet connection almost anywhere in the UK, and even greater bandwidths are being offered too – both things that help IP work even better, and make it an even wiser choice.

So, what do you need to know about IP in order to make it work for you?

First, accept some basic truths

Networks grow - when most clients' networks are initially set up they are small and simple, but very soon they grow and become increasingly complex.

Server location - who knows where the servers are located or how they are supported and powered. Don't assume they are in London's Docklands in a nice clean modern office with 24/7 power.

Downtime - think about what will happen if the client network is down; even the very best system at some time will be off line.

Let's keep things simple

First, let's look at why the old systems need to be updated. Why should you change from the 'good old-fashioned' telephone signalling methods you've come to know?

In my opinion IP signalling will be the de facto standard practice very soon, because the way telephone services are provided is changing. This is making old telephone alarm signalling systems more expensive, less efficient, and in some cases, totally impossible to use.

Within a few short years, PSTN or analogue telephones will be consigned to the past, along with switchboard operators and switched telephone exchanges. BT will continue the roll out of 21CN and the costs of maintaining traditional analogue telephone lines will increase dramatically as a result, making it prohibitively expensive to use them to run traditional alarm signalling. There will be very few cases where a clear case for an analogue connection to the local exchange can be justified. On 'green field' sites and larger buildings the telephone service will be delivered via an IP infrastructure anyway.

A traditional alarm signalling system requiring a PSTN (analogue) telephone line at today's prices could cost up to £170 per year, and even more in future. Whatever type of traditional device is used (unless it's a BT Redcare), part of the way it works will involve making regular check calls, which cost money. The dedicated wiring required adds further costs to the annual bills and additional costs are particularly unwelcome in times of economic hardship.

With IP, an analogue telephone connection is not required as the signalling is sent over the internet in seconds. Plus, line status can be monitored to the class of standard required without all those costly check calls, a positive advantage.

Okay – so IP sounds good! You can now start to see why things need to change with the times, but what should you consider when you are fitting an IP-based system?

How reliable is the client's network?

Firstly, your decisions about whether to use single or dual path signalling will be influenced by how reliable the client's network is, which standards are required (fire, security or both) and the availability/performance required of the system.

When an installer is asked to move a system to IP-based signalling, it should be considered similar in many respects to an in-house or cable network. In the same way as those familiar set-ups, IP relies on external power and third parties to work effectively. This means that for mission critical applications, the network that an IP-based alarm system will be connected to needs careful consideration; it has to be reliable and not prone to crashing, losing power or going offline. Otherwise, the SPT will require a back-up or secondary path over a wire-free connection such as GSM/GPRS over the mobile telephone network.

Some clients, e.g. the Government, NHS and larger financial institutions, operate extremely robust networks these days. They are managed by experts to keep them online 24/7. These highly resilient networks have sufficient capacity and a decent enough infrastructure to ensure that the use of a secondary path may only be needed on rare occasions. Therefore, for simple, yet important, applications such as fire alarm signalling, an IP connection via a managed and monitored SPT to EN50136-1 can be considered adequate.

If such a client's old system had a dial-up connection for the digital communicator in the panel, switching to use a single path connection over Ethernet via IP would be an improvement. As with a digital communicator, there would be no external line monitoring, but a managed IP connection would be able to report a line break appropriate to the risk. However, if the application demanded that 'line fault' be an element in the confirmation profile of an alarm, to comply with EN50131-1/PD6662, then a dual path connection would be essential. An IP-based alarm signalling system that could 'deliver' an alarm over either path and confirm that the alert had been received by those who needed to know about it (rather than just 'send' it) would be vital to ensure compliance.

How secure is the client's network?

You also need to consider the level of security on the client's network. More secure networks will require alarm systems to be added to them in a different way.

For small businesses with direct Internet access over a BT Broadband or similar, the SPT (secure premises transceiver) is a device that can be integrated simply as these sites will employ DHCP server (Dynamic Host Configuration Protocol). DHCP is a simply server application that allows devices to be added to any network with little or no manual intervention, reducing the system administration

workload. Connected this way, the alarm signalling system will work in the background of the client's application; it won't slow anything down as it will add a very small amount of additional traffic to this existing network. In fact, the client will hardly know it's there.

If the client uses a more complex layered network you may not be able to use DHCP. Instead, you might require the network administrator at the company to assign the MAC address of the device you are using to a fixed IP address. Don't worry – this may sound complicated, but it isn't! Any competent administrator will know exactly what you are talking about.

These more complex networks are designed to make sure the administrator can identify all the connections being made within a company's computer system, and see everything that's going on at any one time. This level of control is vital if they are to limit users' access to inappropriate web sites, and protect themselves from invaders. Administrators on such networks will hence be able to see certain details of an alarm system connection, but they have no need to know the geographical location of the SPT so there is little security risk.

This should not be a concern to the installer, so long as a site survey was completed and these details agreed prior to an alarm system being added. Secure signalling providers such as Ascom, as operators of large networked systems, have a customer support team that can liaise directly with a client's network administrator if you have any concerns or need a hand with the tech talk!

How will connectivity to the client's control panel be handled?

Finally, you need to examine how the IP-based alarm system will be connected to the client's control panel, or CIE.

To connect the new alarm system to the CIE, the installer will need to identify a nearby Ethernet connection - ideally within a metre or two of the control panel. You may also need to locate a dedicated power supply if the device cannot share one with the panel, or indeed be powered by the CIE itself.

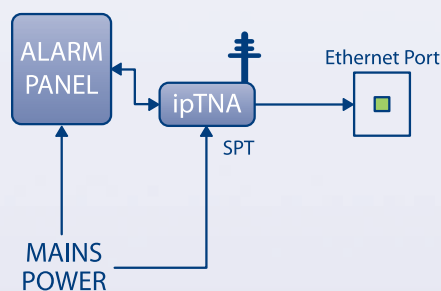
Once this location is identified, you will need to check whether it has a strong GSM/GPRS signal; even if you only wish to use this path very rarely, it's important to ensure a decent long term trouble-free connection and avoid future hassle and re-visits.

SO, your site survey should include this simple checklist:

- Find out what the client's requirements are – the standards they need the system to comply with.
- Determine how reliable their network is.
- Ask the client whether their network can assign a network address via a DHCP. If they have a more complex network and this is not possible, you will need to get the contact details of the network administrator so he/she can assign the MAC address of the device you are using to a fixed IP address.
- Find out where the CIE is located.
- Ensure that a local Ethernet (RJ45) connection or connection to the router is possible.
- Check whether there is a power supply within reach if the CIE can't power the alarm device itself.
- The patch cable must be long enough to reach the Ethernet/router connection.
- Determine the GSM/GPRS signal strength*.

**You can assume that if you are in a sub-surface location or major plant room you may need an external extension aerial, as these situations will limit the penetration of radio signals.*

If you carry out these straightforward checks, using IP should be no more complex than any other type of signalling.



But don't ruin all your hard work by choosing the wrong service provider!

The choice of alarm signalling service providers should also be considered carefully. Revisiting sites is expensive; you do not want to have to make costly journeys to fix problems caused by poor service, especially in these hard times.

Furthermore, let-downs from providers will damage both your clients' and your own confidence in IP systems. That is why it is crucial to opt for a service provider that you can rely on and have confidence in; one with hardware designed for "always-on" operation that won't fail you.

Choose a provider with:

- Experience and high pedigree in secure alarm signalling, with a strong brand reputation to protect – they'll pride themselves in delivering the very best service
- A large bank of testimonials from satisfied customers
- The ability to offer a Statement of Conformity acceptable to regulators
- The resources to support you 24/7
- Connectivity to the ARC of your choice

The average alarm system is upgraded every five to ten years, so you need to be confident that the company providing alarm signalling will still going strong long into the future.

About Ascom

Ascom has been providing mission critical alarm signalling across Europe for more than 20 years, and is supported by a team of more than 2,000 in 17 countries, so they are a very wise choice.

Now you're ready to go! IP is the future.

If you follow the basic principles outlined here - and take up the offers of training from alarm signalling providers such as Ascom - your move to IP will be simple, easy and cost-effective...not only for you, but your customers too.

If you would like to know more about the Ascom range, attend an IP training session, or discuss the cost benefits of moving to IP signalling for you and your customers then do give us a call on:

+44(0)129 354 2030, or email ukenquiries@ascom.com

For more information or a demonstration or visit our UK web site:

www.ascom.co.uk/uk-en/alarmlink.htm