

Warning voice



As BT's 21CN telecoms upgrade to Voice Over IP gets underway, it poses a number of potential problems for alarm installers, says Ian Tredinnick, of IP solutions provider, Chiron Technology. Here he gives his personal view on the changes and urges the industry to be prepared ...



"Be aware of the impending change," says Ian Tredinnick

BT HAS STARTED AN AMBITIOUS £10BN investment in its new 21st Century Network (21CN), which will start to roll out across the UK this year. This will affect all of us in the UK and especially the security industry. The new service is not like ADSL, which is an optional add-on to our traditional telephone services. It's a radical change in the way our telecommunications work and it cannot be avoided, since our underlying PSTN network is being totally replaced.

More importantly, the network behind the familiar telephone socket is changing. Any network problems resulting from this may not immediately be identified and installers and system maintainers could well be looking at their equipment first as being the problem – whereas the change in the network performance could actually be the cause of problems.

All carriers around the world are moving from the old circuit switched PSTN and ISDN systems, to IP-based Voice Over IP (VOIP) networks, which it's claimed will allow customers access to exciting new video-related services such as movies on demand, as well as providing a more reliable and better value telephone service.

The UK is behind most European countries,

which have already moved to VOIP. Interestingly, the security industry over there is already identifying problems.

Over here the security industry finally began waking up, last summer, to a series of inherent drawbacks potentially associated with 21CN. Chiron Technology issued a press release warning that this upgrade of the existing BT network to a VOIP-based one requires the industry to similarly gear up.

(In our September edition we ran a feature written by Alex Carmichael, Technical and Membership Services Director of the BSIA about the potential impact of 21CN and "Welcome to the 21st century" can still be read on our web site www.info4security.com. Just go to the site and key in "Alex Carmichael" in the search box on the right hand side – Ed.)

The rollout of 21CN is far too important to ignore and it is in the security industry's own interests to be aware of the potential downsides – for this is an irreversible switch and will mean System X BT Exchanges are no longer available to handle old digicoms and associated equipment. With the new 21CN network, the old PSTN and ISDN sockets may look the same, but behind them the network, will be completely different and work differently. In fact this will be the main risk, in that many users will not even know their network has changed, therefore problems may not be immediately identified as network issues.

The consequences for installers, who are likely to begin receiving complaints from their customers when incidents start occurring, are serious.

Users of PSTN equipment will not immediately notice any visible difference after BT's network switch has occurred – they will continue to use existing phone line sockets to plug in their equipment to 21CN. But this may lull them into a false sense of security.

The networks behind the new system will change drastically, even though the old PSTN socket may look the same.

The problems are better understood in Europe, where the difficulties of VOIP for security have been seen, but in the UK it is worrying that the change is not understood, or adequate preparation being made.

Some jargon

In order to understand the impact of the new IP networks, as well as 21CN, we firstly need to understand some of the technical jargon that explains why IP is different. For reasons of clarity, I will keep the jargon at the 'top level' and the aficionados who think I am not going deep enough can perhaps save their questions for a later article.

IP is different from other transmission systems such as PSTN or ISDN in that it can cause distortion and errors not inherent in existing systems. There are three different ways in which IP can cause problems, as against PSTN/ISDN. These are: delays, distortion and packet loss.

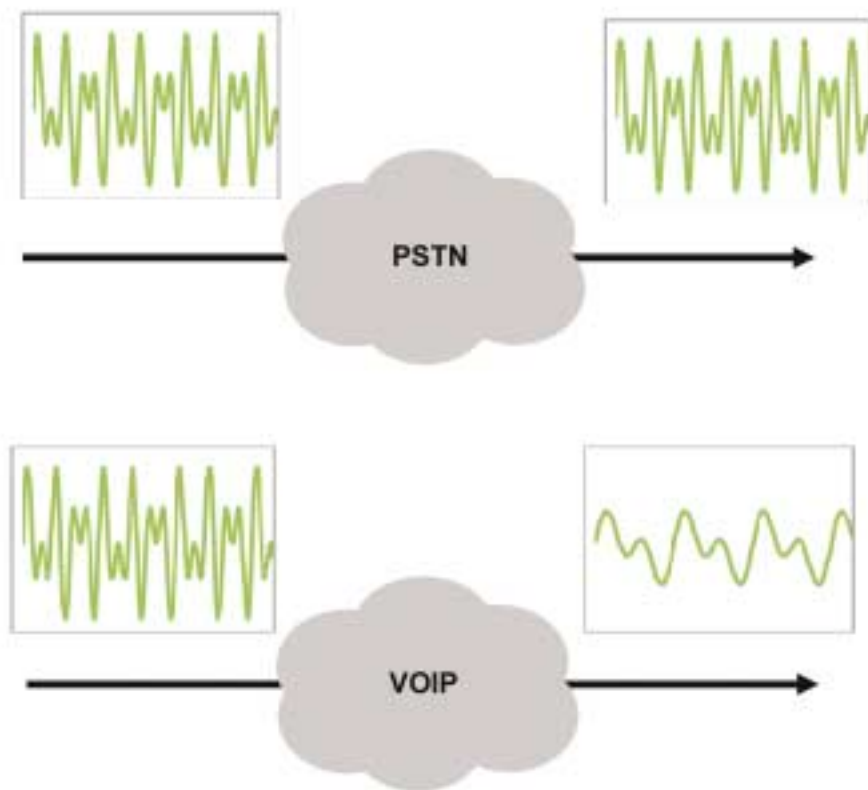
Before we go into these in detail, one has to understand that IP comes in two forms. The first is TCP/IP for data which is fully error corrected, end to end, and this is what has been adopted by all of our data networks. Within this system a delay, or packet loss, will be corrected and overcome. The second form of VOIP, which is part of 21CN, is not error corrected and more suitable to audio traffic such as voice calls.

The new VOIP networks work differently in replicating the old PSTN service across IP and assume that everything is audio, as our ears are very good at overcoming problems such as distortion or crackles. For example, a packet loss would be heard as a minor click in a telephone handset but we would still understand what the person is saying. A word might even be missed, but the brain will compensate. Our alarm panel diallers and their old receivers are not so tolerant. For some applications such as security which, beyond basic uncorrected DTMF/FSK signals, has not moved on during the last twenty years, such a network could cause potential problems. Let us look at the three sources of potential disruption:

VOIP distortion

With PSTN and ISDN, what goes in at one end is then repeated as it comes out the other end, with no delays or distortion. We have used these systems for years with extremely low alarm failure rates, which represents the quality and reliability of the old carrier mechanisms rather than any failures in the alarm equipment within the premises. Fig. 1 (overpage) shows the

Fig 1: Signal distortion over VOIP network



comparison of a PSTN or ISDN signal with what may be expected across VOIP. Within the security industry, our traditional receivers look for a very regular shaped pulse. However, VOIP in its conversion from analogue to digital and back again can potentially distort this signal, as shown. Already we have proven cases on 21CN where existing PSTN receivers used widely within the security industry are rejecting calls coming across VOIP networks due to distortion of the pulse.

This does not mean every call will be rejected, but the potential is far higher than on current networks. The fact is that the new alarm alert could be rejected and lost.

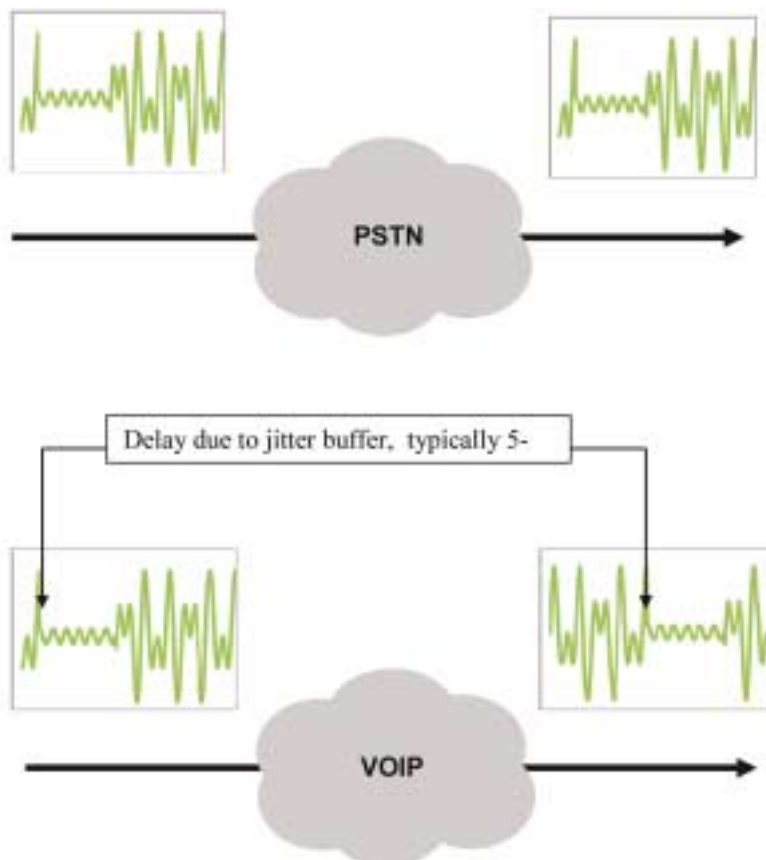
BT's 21CN uses high quality codecs, so this problem should be minimised. However, once we adopt the principles of VOIP calls from other ISPs who may not use the same standards, then these problems may increase. Our industry cannot today rely on the BT monopoly, as there are an increasing number of carriers, and we will not know how many networks our calls have passed through.

Delays

We are all aware that transient delays can occur within an IP network. If these delays happen between pulses (see Fig. 2), then the receiver can once again reject the call as it is looking for a number of strict timing limits and pulses. BT's 21CN will attempt to overcome this by the introduction of what is called 'jitter buffers'. This is where they insert an overall delay of 10 milliseconds. The idea of this is to overcome any transient delays during the duration of the call. Whilst this is a good idea to reduce errors, it can give the security industry a number of problems:

It may interfere with the overall timing response required between security panel and receiver. Also, once this buffer is used up for the

Fig 2: Signal delay over VOIP network



duration of the call, then BT will introduce blank packets into the message stream. A standard receiver will interpret this as an error. This will cause a rejection by the receiver in what could be a potentially urgent alert.

Packet losses

This is the most important and potentially dangerous aspect of IP networks to the security industry. Packet losses can occur anytime and anywhere within the network.

Quite often they are transitory and do not stay long. For example, we are all used to accessing a web page which on one occasion will appear immediately and then if we try ten minutes later, might have delays in coming up on our screens.

For error-corrected TCP/IP systems this is not a problem, but for basic uncorrected DTMF/FSK alarm signals then a VOIP call will almost certainly cause an alert failure on traditional PSTN receivers.

The major problem of these packet loss problems being transitory is that they will come and go at different times in different places.

A full error corrected TCP/IP security system will identify packet loss and retry using the network's resilient alternate routing mechanism. VOIP will not, however, and the resultant packet loss will be seen by the receiver.

This will happen with 21CN, but the real question is how much and in what circumstances?

So let us move on to look at the practical effects of these three potential VOIP problems. These problems are manifested in the form of interference and loading.

Currently, on a lightly loaded network they are unlikely to cause problems to security or any other

application. But BT says that 21CN will not be a problem, as it is designed to cope with packet losses of 10-8. The company would have us believe that a packet loss of one in 10,000,000 is adequate. However, this is an average and does not take into account peak period problems. In addition, we need to look behind this impressive figure. During peak loading, how many calls will BT be maintaining sequentially?

It is likely that there will be in excess of 20 million packages per second flying around 21CN. This means we could be losing, on average, three packets per second across the network, doubling, trebling or more during peak periods.

Obviously, some of these will be alarm alerts. The question for our industry is "what is acceptable?" because these losses and delays of VOIP will be many times more than we have experienced in the past. Some security manufacturers and ARCs have already identified problems with legacy equipment on the 21CN test system. If we are having problems today, then as soon as we get a loaded network with a greater degree of congestion, these problems will be magnified enormously.

What do we consider as acceptable? When I say "we", I mean everybody in the security sector: manufacturers, monitoring centres and ARCs and, especially important, the insurers. This will affect all of us.

In light of the above, I understand that BT started to roll out 21CN in parts of Wales during the end of 2007, with Cardiff being switched over

in early 2008 and the rest of the UK following in the years up to 2012. Once BT has switched to 21CN, there will be no going back. On the live network there will be no divers for security applications and no bypass for our industry, as has occurred during the trial period.

Thoughts for the security industry

BT is giving us assurances that 21CN will not be a problem. Hopefully it is correct. But indications from other European countries, which are ahead of us in the use of VOIP, are that the path will not be as smooth as BT would lead us to believe. It is extremely concerning that there has been no testing of a loaded network in the UK and the participation of the security industry has been minimal and late. There has to be an urgent choice made about what level of risk we are able and willing to accept, and what error rate and packet loss, if any, is acceptable. As part of this process, the insurers should, at least, be involved or aware of the potential implications.

New technologies

There are IP products available which overcome the potential problems by VOIP, offered by my own company and other companies. However, I would recommend that the industry as a whole needs to look closely at this new 21CN activity. It cannot be avoided, it cannot be swept under the carpet and it cannot be ignored. If there are major problems with the rollout in early 2008, it could hit our industry hard and quickly. If problems do

surface, the major question is: Could we even re-equip and re-configure all of the signalling equipment within the alarm panels in the market today to keep up with the pace of BT's changeover?

Conclusion

So what should security installers, insurers and monitoring centres do now? In short, make sure that the technology you use is robust and will operate over the planned VOIP network. Dual-path IP/GPRS systems meet this criteria. Anyone who ignores this issue on the principle that 'things will be OK most of the time' is leaving their system open to failure. It is up to the security industry to be aware of the impending change to our underlying methods of working which cannot be avoided.

About the company

Ian Tredinnick, is MD of Chiron Technology, Wyvois Court, Swallowfield, Reading, RG7 1WY. Tel +44 (0) 118 988 0228, Fax +44 (0) 118 988 1055 or email ian@chiron.uk.com. The company's security products are now used in a number of applications, such as connecting standard panels to ISDN, dual path signalling, video surveillance, alarm connections over private IP networks etc. The company's IP solution, the Iris system, is based on full TCP/IP error protected protocols.