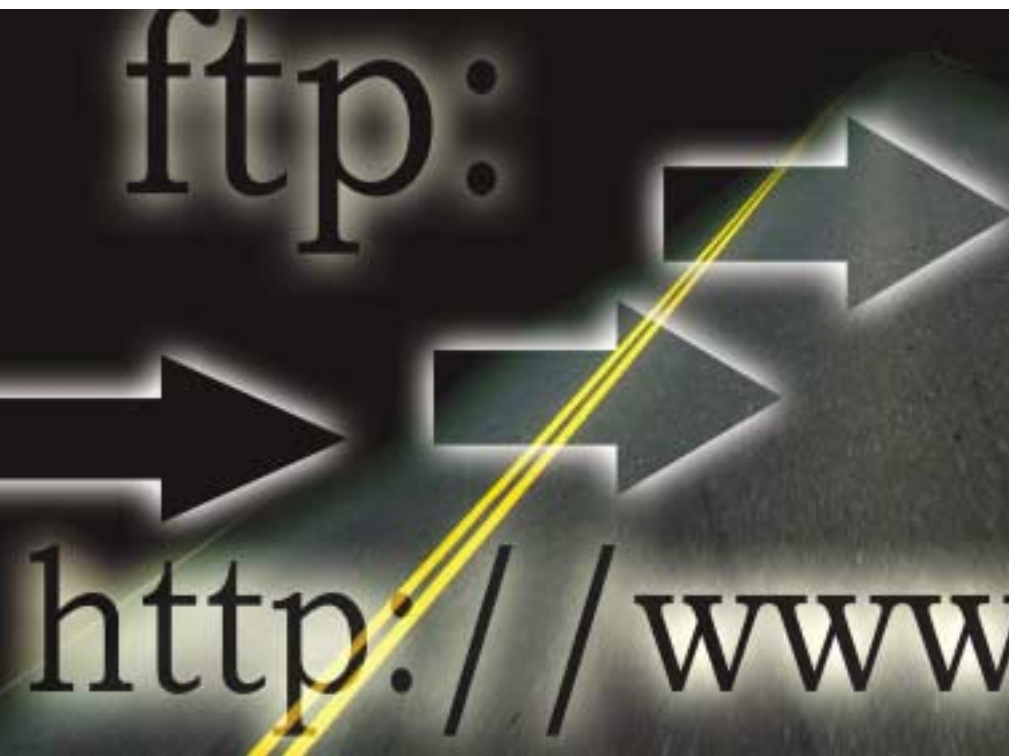


# This is the 21st Century



**BT's bold £10 billion 21st Century Network (21CN) Project represents a radical change in how our telecommunications systems will work, involving a switch from PSTN to Voice-over-IP. Is that change going to come at a price for end users? Ian Tredinnick explains why the transitional path may not be quite as smooth as BT would have us believe. Illustrations courtesy of EuroStyle Graphics/Coston Stock/Alamy Images**

THE USE OF IP NETWORKS FOR ALARM SIGNAL transmission and monitoring has been shown to be effective and reliable for many end users – clients who stand to benefit from advantages including the significant operational cost savings involved, improved network resilience and added value services.

As highlighted by your journal, travel chain Thomas Cook is but one example of a business where comparative monitoring cost savings of 70% per annum have been achieved without compromising security ('Moving towards IP monitoring', Briefing Papers, SMT, December 2006, p45).

Last year, we saw the first signs of the UK security industry finally waking up to the potentially serious consequences of a related move that will affect all of us on home shores. I'm talking here, of course, about BT's ambitious £10 billion 21st Century Network (or 21CN) Project. The new service isn't like ADSL, which is an optional add-on to our traditional telephone services. Instead, 21CN represents a radical change in the way in which our telecommunications work, involving a switchover from PSTN to Voice-over-IP (VoIP).

Last summer, Chiron responded to a press statement issued by the British Security Industry Association (BSIA) in underlining the fact that this upgrade to the existing BT network requires the security sector to 'gear up' in tandem. End user customers and others – including security planners, insurers and the Alarm Receiving Centres (ARCs) – need to understand (and quickly) how their systems may be affected, and what they can do about it.

## **Irreversible one-way switch**

Chiron's experience to date in other European countries (such as those in Scandinavia, which are ahead of the UK when it comes to adopting VoIP) indicates that the path to this new transmission network will not be as smooth as BT would have us believe. VoIP can make alarm alerts unreliable and render uploads/downloads very difficult. It has also been found to adversely affect credit card technology, social alarms and security alarms.

The problems with transmission may be unpredictable and only occasional, but where critical systems are concerned even occasional data loss is completely unacceptable.

Data carriers around the world are moving from the old circuit-switched PSTN and ISDN systems to VoIP networks because they offer the marketing and revenue-related attractions of customer access to new video-related services (such as movies on demand), at the same time providing a more reliable and better value telephone service.

To achieve the delivery of these new services, all network operators are installing VoIP infrastructures as they allow higher IP transmission speeds to be achieved. However, end users ought to be aware that this is an irreversible one-way switch, with System X BT Exchanges no longer being available to handle old digicoms and associated equipment once the move is completed.

Deceptively, the old PSTN and ISDN sockets may look the same when using 21CN, but behind them the network is completely different and functions in a dissimilar fashion.

Indeed, this will be the main risk. Many users will simply not even know the network has changed, and operating problems may therefore not immediately be identified as network-related issues.

The problems discussed here are better understood in Europe, where the difficulties surrounding VoIP for security have already been witnessed. In the UK, it's massively worrying that not only is the upcoming change [to 21CN] not understood, but there's also a lack of adequate preparation.

## **IP: in two formats**

VoIP is different from other transmission systems such as PSTN or ISDN in that it can cause distortion and errors not inherent in existing systems (including delays and packet losses). Before examining these errors, it should be recognised IP comes in two forms.

First, TCP/IP for data that's fully error-corrected, end-to-end. This type has been adopted by all of our data networks and, within this system, a delay or packet loss will be corrected and overcome. The second form of VoIP – which is part of 21CN – isn't error-corrected, and more suited to audio traffic.

The new VoIP networks operate differently in replicating the old PSTN service across IP. They assume that everything's audio, as our ears are good at overcoming problems like distortion or crackles. For example, a packet loss would be heard as a minor click in a telephone handset, but we'd still understand what the person is saying. A word may well be missed, but the brain compensates.

Our alarm panel diallers and their old receivers are not so tolerant. For some applications like security – which, beyond basic uncorrected DTMF/FSK signals, hasn't moved on during the past 20 years – such a network could cause potential problems.

With PSTN and ISDN, what goes in at one end is then repeated as it exits 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).

Within the security sector, our traditional receivers look for a very regularly-shaped pulse. However, during its conversion from analogue to digital and back again, VoIP can potentially distort this signal. Already, we have proven cases on 21CN where existing PSTN receivers used widely within the security industry are rejecting calls sent across VoIP networks due to this distortion of the pulse. This doesn't mean every call will be rejected, but the potential for that occurrence is far higher than is the case with current networks.

## Will the 'jitter buffers' work?

The fact is that the new alarm alert could be rejected and lost. BT's 21CN does make use of high quality codecs, so the problem should be minimised. However, once we adopt the 'workings' of VoIP calls from other Internet Service Providers (ISPs) who may not use the same standards, then these problems may increase. Our industry cannot rely on the BT 'monopoly' as there are an increasing number of carriers, and we'll not know how many networks through which our calls have passed.

We're all well aware that transient delays can occur within an IP network. If these delays happen between pulses, then the receiver can once again reject the call as it's seeking a number of strict timing limits and pulses.

BT's 21CN will attempt to overcome this by the introduction of what have been termed 'jitter buffers'. These insert an overall delay of ten milliseconds. The idea of this is to overcome any transient delays over the duration of the call. While this is a good idea for reducing errors, it can realise a number of problems for the security industry.

It may interfere with the overall timing response required between security panel and receiver. Once this buffer is used up for the duration of the call, then BT will introduce blank packets into the message stream. A standard receiver interprets this as an error. This will cause a rejection by the receiver in what could be a potentially urgent – maybe even life-threatening – alert situation.

## Packet losses: a major concern

Packet losses are the most important and potentially dangerous aspect of IP networks as far as the security industry's concerned. They can occur at any time and anywhere on the network. Quite often they're transitory, and don't stay long. We're all used to accessing a web page which will appear immediately and then if we try again ten minutes later there might be a delay in it appearing on our screen.

## "The problems with transmission may be unpredictable and only occasional, but where critical systems are concerned even occasional data loss is completely unacceptable"

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

### ...but 21CN will not be a problem...

The major difficulty with these packet loss problems being transitory is that they'll 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, though, and the resultant packet loss can be seen by the receiver. This will happen with 21CN, but the real questions are how often is this going to occur and in what circumstances?

Moving on to the practical effects of these three potential VoIP problems, they're manifested in the form of interference and loading. Currently, on a lightly loaded network they're unlikely to cause problems for security or any other application. Using its mega PR machine, BT is trying hard to tell us all that 21CN will not be a problem, as it's designed to

cope with packet losses of  $10^{-8}$ . BT would have us believe that a packet loss of one in 10,000,000 is adequate, but this is an average and doesn't take into account peak period problems in any way, shape or form.

We need to look beyond this 'impressive' figure. During peak loading, how many calls will BT be maintaining sequentially? Two million? Four million? More? It's likely there'll 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. That figure could double, treble or increase even more in peak periods.

Obviously, some of these will be alarm alerts. What's acceptable, because these losses and delays associated with VoIP are going to be many times more than we've experienced in the past? Using one of the properly designed and error-corrected TCP/IP security systems will overcome the vagaries of 21CN.

What's even more worrying is that all trials of security equipment carried out by BT have only been conducted on lightly loaded test networks. Even then, some security manufacturers and ARCs have identified problems with legacy equipment.

## Testing of a loaded network

In light of the above, we understand that BT is already rolling out 21CN in parts of Wales, with 350,000 lines in Cardiff being switched over in 2008 and the rest of the UK following in the years to 2012. BT is giving us assurances that 21CN will not be a problem, but it's extremely concerning that there has been no testing of a loaded network in the UK and that participation of the security industry has been minimal.

Both BT and the BSIA assure us that they're currently working together on a test plan that fully reflects the needs of security communications requirements on the 21CN platform. "Many hundreds of hours of testing" are said to have taken place, identifying concerns that the two organisations are now investigating to produce solutions.

The manufacturers of communication products and ARC receiving equipment are reported to be fully engaged in this process to ensure that equipment will work on the 21CN platform, and also to see how the transition to 21CN can minimise the effect on those legacy products that have been installed.

End users must be aware of the need for an alternative solution to VoIP. This comes in the shape of dual path IP/GPRS systems. Here, essential data does make it through to the recipient – one way or another. ■

■ Ian Tredinnick is managing director of Chiron Security Communications (part of the Chiron Technology Group) ([www.chiron.uk.com](http://www.chiron.uk.com))

"In the UK, it's massively worrying that not only is the upcoming change [to 21CN] not understood, but there's also a lack of adequate preparation"

