TSA™

The voice of technology enabled care

THE IMPACT OF ANALOGUE TO DIGITAL MIGRATION ON TECHNOLOGY ENABLED CARE – January 2021

KEY FACTS

>> The Technology Enabled Care Services Association (TSA) is recommending that service providers take urgent action to review the impact on their alarm services of the transition to digital telecommunications infrastructure across the UK.

>> The so-called 'All IP' (All Internet Protocol) data and voice services are already being deployed, and they will accelerate during 2021.

>> BT Consumer division has already extended its criteria for Digital Voice customers to include the 'special services' provided by the TEC sector.

>> Service providers are likely to start receiving enquiries from users about the impact of the telecommunications changes.

What's happening now?

The UK Communications Providers (Openreach, BT, Virgin Media, TalkTalk, Sky etc.) are transforming the telecommunications network in the UK from the traditional phone-line system to one which is based entirely upon the movement of 'packets' of digital information (so called 'All-IP' networks). This relates to the increasing difficulty of maintaining older networks, but it is also driven by our desire for faster networks and the insights than come with enhanced connectivity of citizens to information and services - the change should be viewed as an opportunity for service re-design and improvement.

By December 2025, the majority of UK businesses and residential premises will be accessing high speed connectivity for voice and data services in place of phone line technology. Premises may migrate entirely to optical fibre infrastructure or to a mix of both copper and optical fibre, depending on geography.

What will be the impact?

All voice calls (including analogue alarm calls and data) will no longer be able to use traditional phone networks.

All such communication will need to take place via devices connected to a router and over an internet protocol (IP) network, or via mobile networks. This changes the way that existing alarm systems operate.

The take up of the digital services has been sporadic so far, and limited to pilot trials in Salisbury, (Wiltshire) and Mildenhall (Suffolk), where the Openreach exchanges have been migrated to 'All-IP' technology.

Where ALL-IP infrastructure exists, no new 'analogue' phone lines will be installed after Dec'20 in Salisbury and May'21 in Mildenhall and a further 168 exchanges are already planned for migration to All-IP during 2021.

The systems and devices employed in the TEC sector should be migrated quickly to technologies which are **designed to operate reliably over digital landline and/or mobile networks,** whilst meeting relevant product standards. However, it is also recognised that the operational and financial impact will cause some service providers to seek **phased responses** to these changes, where the greatest risks or most vulnerable technologies are addressed as a priority.

TSA has therefore gathered the opinions of UK service providers on their needs for assurance on the reliability of telecare and social alarm systems as we shift to 'All-IP' networks. This involved the creation of a Special Interest Group under the TSA Quality Improvement Programme, which captured a set of requirements during 2020 and which are summarised in this paper. Some of these requirements can be related to the need for testing of alarm systems over new communication networks, whilst others are best described as risks that need to be addressed.

Action: Service providers take urgent action to review the impact on their alarm services of the transition to a digital telecommunications infrastructure, and to include consideration of the issues summarised in this paper.

1. RISK MANAGEMENT ISSUES

A number of issues were identified by the analogue to digital Special Interest Group (SIG001), which should be included in your risk management and contingency plans. As follows:

1.1 Upgrade or Migration Funding

Inevitably, service providers have identified their concerns that large-scale equipment replacement or upgrade may be needed. The newer, digitally enabled equipment may also come at significantly higher price points than previous analogue equipment, at least initially, and often comes with ongoing monthly charges. This all presents a commercial risk that needs to be managed.

1.2 Interaction of Vulnerable Users with Communications Providers

Communications Providers are making special efforts to manage 'vulnerable users', in terms of their sales and installation processes. However, alarm users do not automatically qualify as vulnerable, and users need to register as such with their communication provider.
Initially, BT filtered and blocked All-IP upgrades for alarm system users. This situation has changed, and BT now refers such users to their alarm monitoring service to seek confirmation that alarm equipment is compatible. Monitoring services can therefore anticipate a growing number of queries from users.

Also, communications engineers are being advised not to re-install or re-check any connected devices (e.g. alarms) when installing new digital connections in homes, and they plan to abandon any installation where a user may be put at risk. Alarm service providers will need to respond to queries that arise and any necessary re-connection and testing.

1.3 Digital Skills and Workforce Development

A number of TSA studies over the last 24 months have highlighted that we need to consider the level of digital awareness and skills amongst our workforces. This ranges from the ability to respond to queries from users about home alarm connectivity to the best practice that is relevant to data protection and cyber security.

1.4 Power Failure Protection

EU and hence UK social alarm standards currently require 24-hour continued operation in the event of local power failure. Importantly, traditional phone lines still work and are powered even when home power supply fails. However, communications providers do not provide this facility on their digital connections. The automatic notification to monitoring centres of loss of power to alarm devices will also be lost. Furthermore, Ofcom regulations for All-IP only require

Action: Service providers will need to assess the risks and their liabilities given this lack of continued standards compliance for alarms that connect via landline only.

1-hour continuity of access to ‘999’ services for ‘vulnerable users’ in the event of power failure to the home (loss of power leads to home ‘router’ failure).

Is there a workaround?

Communications providers are addressing the 1-hour continuity challenge in different ways. For example, one Communications Provider plans to supply a separate back-up device for 999 calls only, and it does not support alarm products. The device connects over mobile networks, and it is to be used only in the event of local power and/or router failure. Consumers need to be aware of and able to use such a back-up product in an emergency, and they also need to be assured of plans for suitable maintenance (charging, fault monitoring, servicing). It should be noted that battery back-up products will generally be provided free of charge only to users who are registered as vulnerable.

Some other countries (e.g. Sweden, Germany) have amended their social alarm guidance to adopt mobile connections as primary or secondary communication paths for alarms, and the UK may follow.

1.5 Access to 999 Services

The impact of power failure highlights that we need to ensure access to emergency services is available for monitoring services and end users. Monitoring centres typically escalate 2%-5% of all incoming social alarm calls to emergency services for resolution of incidents.

Action:

(1) Alarm service providers will need to review their Business Continuity Plans to ensure they can still connect with emergency services in the event of local power failure and/or loss of primary communication networks.

(2) Alarm service providers should ensure that users are aware of the impact of All-IP and local power failure on 999 access and alarm services, as vulnerable users may also make use of 999 services in the event of emergencies, in addition to their alarm service.

1.6 Impact on Non-Geographic Telephone Numbers

Alarm devices typically use both geographic telephone numbers (beginning 01 & 02) and non-geographic numbers (e.g. beginning 07, 08), to provide diverse or back-up calling options. It is not yet clear whether these same options and benefits will persist under All-IP, so business continuity plans need to be re-examined.

1.7 Impact of New Communication Types

New alarm products are emerging which employ different combinations of fixed-line and mobile connections for each of their data and voice paths. Mobile connections also come in different flavours, using 2G to 5G variants, and some products retain analogue connections rather than digital for voice, and all carry ongoing monthly charges. Many alarm unit manufacturers have developed alarm units that only operate on 2G/3G cellular bands and, whilst the actual date of switch-off of these networks is unclear, the major communications providers are expected to switch-off these networks in favour of 4G/5G at some stage.

Action:
Service providers need to consider the impact of these communication types and the projected product lifetimes.

1.8 Peripheral Devices

Alarm units in the home are generally connected to wireless or wired peripheral devices and sensors such as pendants, smoke detectors, fall alarms, bed sensors, door sensors etc. Unfortunately, alarm peripherals are generally not compatible from one manufacturer to another. This means that if digital upgrades require the changing of alarm units then Service Providers will face the additional capital cost of replacing peripheral devices. There are also examples of manufacturers providing new alarm units that are not backwards compatible with the alarm peripherals that link to older equipment.

Action:
Services will need to check the impact of digital upgrades on peripheral and sensor devices.

1.9 Product Compatibility and Procurement

The limited interoperability of equipment between suppliers across the end-to-end alarm chain has been a historic concern for alarm systems, since this presents obstacles to user choice and to best-value procurement. Service providers in the Analogue to Digital Special Interest Group have highlighted the need to address this issue as we 'shift to digital'. Specifically, suppliers of alarm equipment and monitoring centre systems need to share communication specifications openly, including methods of signalling and protocol exchange (the message structures). Monitoring centres should include access to open communication protocols which have been proven to support digital alarm voice and data. Similarly, suppliers of any connected alarm products need to confirm which of the communication options they provide. This includes details of the networks they will operate with (fixed-line and mobile variants 2G/3G/4G/5G) and the communication protocols implemented. Successful integration can also be impacted by details of configuration.

Action:

(1) service providers seek evidence that suppliers of monitoring centre and alarm technology have engaged in mutual compatibility testing.

1.10 System Resilience

It is expected that the shift to All-IP could impact significantly on the configuration of alarm systems and monitoring centres, and therefore service providers will need to re-evaluate the reliability and availability of their end-to-end systems. It should also be noted that concerns for cyber security are heightened by the anticipated 'shift to digital', as identified by TSA's recent study on data protection and cyber security in the TEC sector. TSA has previously provided relevant guidance information, including:

- Digital Readiness Guidelines
- Mobile Communications Guidance
- Data and Cyber Security

1.11 Equipment Withdrawal

We are still in the early days of digital transition, but there are already reports of older equipment (e.g. 'pulse dialling' and some 'tone-signalling' equipment) failing on digital networks.

Action: Any equipment which does not fall into the category of 'supported' should be withdrawn from service as soon as possible. Supported products are those which are declared by manufacturers as fit for purpose on All-IP networks, or supported by ongoing repair and maintenance services, or still in manufacture. Any unsupported products should be planned for withdrawal and replacement as quickly as is feasible.

1.12 Inadvertent Impact of Alarm Functionality

Phone-line connected telecare alarms include a range of functionality which may impact in different ways over All-IP networks. Service providers, supported by their technology suppliers, need to assess the impact and risk of such functionality, including:

- **Off-hook override**: The ability of alarm devices to identify connected telephones as 'off-hook', and then give priority to alarm devices is unlikely to be supported in All-IP home installations.
- **Power loss alerts**: Alarms generally detect loss of power and alert monitoring centres and users. Service providers need to make sure that such alerts are still appropriate and effective.
- **Phone line loss alerts**: Alarms generally detect loss of phone line and alert users. Service providers need to make sure that such alerts are still appropriate and effective. A particular concern here is that All-IP routers may need to upgrade regularly (and overnight)

presenting a loss of phone line condition and requiring that consumer alerts be managed at scale.

2. ANALOGUE TO DIGITAL TESTING REQUIREMENTS

Service providers have expressed concerns for the existing 1.8 million (Fagerberg, 2019) connected UK users of telecare alarm services. It is estimated that over 1.3 million relate to single home use, with the balance employed in grouped living housing environments. Virtually all these systems rely on remote connections to Alarm Receiving Centre services, and they currently employ phone-line connections in the vast majority of cases.

The TSA sponsored Special Interest Group concluded that where services have considered and mitigated the identifiable risks, and where they have justified the continued use of 'analogue' alarms and receiving centres during a transition period, then all such product variants need to be tested. The working group identified the following key requirements to be included in any testing of 'analogue' alarms over new communications networks:

2.1 Clearly identify the equipment that is tested

Any products which are currently supported (see 1.11) need to be tested.
Testing needs to be specific in terms of the system and equipment under test, including model and version identification of both the monitoring centre system and the connected alarm product, the type of communication protocol employed and the details of any necessary connected devices (such as analogue telephone adapters).

2.2 Product testing requires independence

Service providers have requested that product testing is verified independently of the product suppliers. As a minimum this would require independent review of the test configurations and results.

2.3 The scope of testing needs to be realistic and representative of real-world conditions

- The end-to-end alarm chain needs to be tested across multiple network types – an alarm user may for example use BT, but a monitoring service may be contracted with Virgin Media. So, the testing needs to include combinations of at least two different communications providers and their various analogue or digital connections. An underlying concern here is that 'gateways' between different network types may pose the greatest risk to reliable transmission of alarm data tones during the staged migration process.
- Equipment testing needs to include in-call data messages (such as volume control, speech switching, call clear-down, remote programming).

- Grouped housing alarm systems typically employ their own communication networks within a housing scheme (either analogue or digital), but they also connect remotely to monitoring services in different ways. So, the various grouped housing systems or configurations need to be included in the testing.
- Variable network performance is a concern, since digital alarms may share networks with lots of other data, voice and video services. This means that testing needs to cover a range of impaired conditions that could result from network loading. The technologists refer for example to variable 'packet loss' and 'round-trip delays', which need to be adjusted in the testing, to represent nominal and 'worst case' network conditions. A challenge here relates to the extent to which network parameters can be configured at test facilities.
- Alarm devices employ clever functionality when operating over traditional phone line connections. For example, analogue alarms try to ensure the reliability of their calls by making multiple attempts when exchanging data within a call, or re-dial attempts and even call re-direction to other receiving centres in the event of alarm failure. However, these mechanisms can add significant and potentially unacceptable delays to alarm call handling, and therefore any test outcomes need to capture such events.
- Some Alarm Receiving Centres have volunteered to help with multiple product and network tests. However, their resources will be constrained, given their continued commitment to alarm services, and this resource needs to be coordinated and managed carefully.

2.4 Good and Open Communication

Providers of receiving centre and alarm technologies need to be prepared to share their test results openly. TSA has volunteered to coordinate common methods of communication, and this would be guided by an independent working group.

Next steps?

TSA recommends that service providers take urgent action to review the impact on their alarm services of the transition to digital telecommunications infrastructure across the UK, and to include consideration of the issues summarised in this paper. TSA will endeavour to provide support to services in addressing further issues that arise.

The so-called 'All IP' (All Internet Protocol) data and voice services are already being deployed, and they will accelerate during 2021. BT Consumer division has already extended its criteria for Digital Voice customers to include the 'special services' provided by the TEC sector. **This means that service providers should anticipate and plan for enquiries from their users about the impact of the telecommunications changes.**

Get in touch

The onward development of guidance material on these topics will continue through TSA Special Interest Groups, and contributions and involvement from service or technology providers are welcome, please contact TSA at admin@tsa-voice.org.uk or 01625 520320 to express your interest.