TEC Services Association

Mobile communications guidance

Guidance for providers of TEC services on the use of mobile connectivity

Contents

Introduction

As the world moves away from analogue phone connections, and some limitations of digital broadband during this transition are becoming clearer, Mobile, delivered correctly, becomes a strong option for a reliable and secure Telecare connection.

In Telecare, it is naturally assumed that the hardware/devices should adhere to strict standards and testing in order that they function in those critical moments. It is equally expected that the Alarm Receiving Centre runs appropriate monitoring platforms and software, is staffed appropriately, so that the incoming call can be answered quickly, effectively, and securely. With that in mind, it seems only logical that the way in which these two critical parts of the Telecare system are connected, is vitally important, yet currently no standards or regulation are available to guide on how to ensure that this is done correctly in a digital world, for in the mobile world, not all SIMs are created equal.

Much of the history of Technology-Enabled Care stems from telecare and precursor social alarm systems. Even today, the majority of the UK's 1.7 million users of TEC systems are connected to their care services via telecare. These systems are dominated by home-based alarms or hubs, linked to alarm receiving centres, and have made good use of trusted, analogue phone lines to exchange voice calls and limited but critical data. The assumptions that relate to these technology solutions have been embedded over time in standards (such as the EN50134 series) and corresponding service expectations.

The TEC landscape is evolving.

Technology-Enabled Care systems are expanding from telecare to include telehealth, social inclusion, self-managed care, digitally-connected devices around the home and a range of mobile solutions.

Telecommunications networks are changing too, migrating from analogue (TDM) networks to digital networks that see only packets of IP (internet protocol) data. Previous assumptions relating for example to network availability, voice data reliability and power back-up are all being challenged by new potential failure issues.

A wide range of new, digital technologies are emerging, including wearable devices, Internet of Things, cloud hosted applications and more. This is a world where we can anticipate many new solutions, and where existing standards or guidelines that prescribe particular design solutions will increasingly appear outdated.

In this environment, care providers will seek and find a widening spectrum of technology-enablement that could benefit their service delivery. We can expect that regulatory standards will need to be abstracted from statements of how systems are constructed, to focus instead on what service capabilities they need to enable. We will see greater emphasis on the availability of systems when needed, resilience and recovery in response to failure, capacity and performance when stressed. It will then be for suppliers to demonstrate how their varied systems deliver against these requirements.

TSA is working with standards development organisations (such as CEN, CENELEC, BSI) and care regulators to help navigate these changes, and to help adapt the framework of standards for technology-enabled care. The shift away from prescriptive (design) standards will inevitably create opportunities for innovation and a wider spectrum of TEC solutions, and where users and providers of services and technology will hopefully appreciate advisory content from experts in the field and from adjacent industry sectors.

With this in mind, the TSA and its Technical Advisory Group is working with members and other contributors to create a range of guidance materials. What follows is a guide to mobile connectivity in Technology-Enabled Care, a subject that will grow in importance as we adopt mobile and wearable care devices, and where cellular networks offer diversity and redundancy in a changing telecommunications environment.

Points to consider

Why use Mobile Networks?

These guidelines will give you a better understanding of working with Mobile Networks, the 'gotchas' and what to look out for, along with some general tips and advice.

Increasingly there is a need to connect Telecare users without access to traditional phone lines and prepare for when digital mobile networks are implemented as a primary or backup connection. Properly applied, Digital Mobile Networks for Telecare use offer excellent reliability for voice and data.

Many people consider mobile networks as just voice and data, and do not realise that there are also dedicated Internet of Things (IoT) mobile networks. These networks differ from the normal view of mobile communications, as they offer no conflict of text and voice but provide controlled internet access and 2-way communication through dedicated data networks and site-to-site interconnects or Virtual Private Networks (VPNs). This increases the security of the network without the added data and cost that a device to server VPN, or over the air VPN creates.

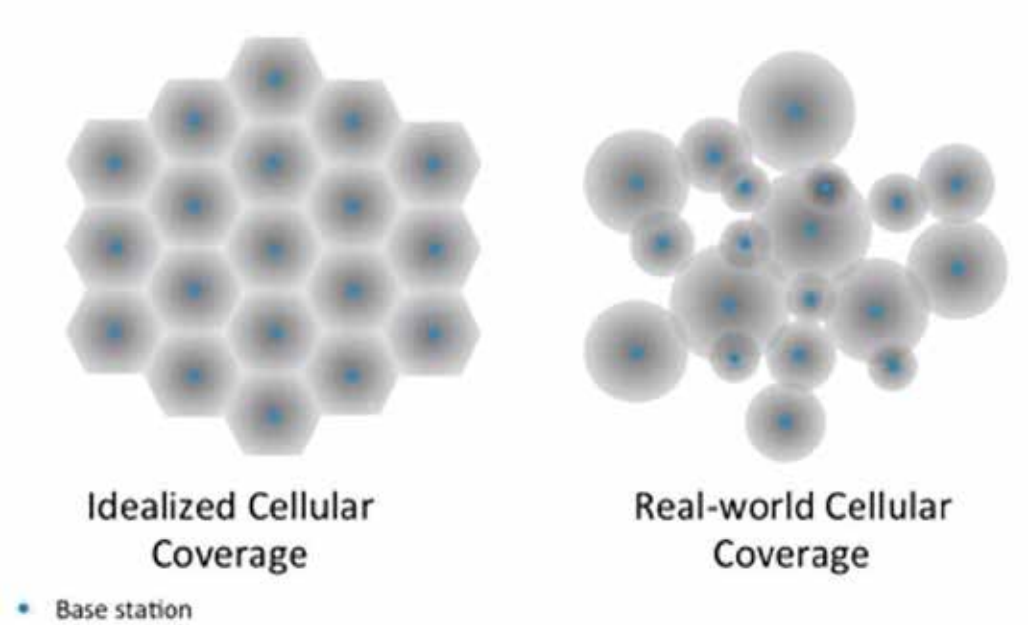
C Helpful Advice

An issue that often is not picked up on is the networks' tendency to round to the nearest 1KB of data per transaction. This is fine if files are of the order of KB or MB but many TECS transactions are themselves only tens of bytes. Very often the lack of aggregation and the charging for lost SIMs also pushes costs up far higher than an initially calculations would suggest. Therefore it is best to seek out a provider who bills to the byte.

1. Network connection and device issues

1.1 Cellular coverage & antennae

You can save hundreds if not thousands of pounds and countless hours of engineers' time by investing in a good antenna for a connected device. It is often the difference between the site working well and the site being viewed as failing. Approximately 1% of installations could require a "high gain" antenna to enhance coverage in less covered regions.



Mobile networks cells are constantly changing. A cell will create a donut shaped signal area and anything in that donut will get a signal, but this signal gets weaker the further away from the cell you go. As a user connects to a cell the size of the footprint shrinks. If you are at the edge of a cell and it shrinks you will no longer have a connection to that cell and you will connect to another cell that is also serving your location if there is one, or you will drop to another technology, such as 2G/3G.

The weather also affects cells as do trees and buildings with modern buildings being particularly bad for mobile networks as the mix of glass, steel and foil backed insulation scatters, reflects and absorbs the mobile signal.

Cutting corners with the antenna can cause huge dips in the performance of the connected device.

1.2 Network or cell is down

It is true that mobile networks and cells do experience loss of coverage. However this is planned and generally takes place overnight and in very specific locations. When things come back up it is generally the poor set up of the equipment that prevents these events passing seamlessly, as often the equipment still regards its last session prior to the disruption as active and is unable to recover from this state without human intervention (manual reboot). In most events, the TEC device will have access to another Mobile Network Operator (MNO) network in order to continue to function, but the device needs the intelligence to ensure it is selecting the best network at any given time.

The mobile network providers have invested heavily in their networks, improving the cell densities within the towns and cities (greatly reducing the number of 'network busy' messages) and covering more and more of the UK land mass. Within most urban environments it is common for a mobile device to see up to 50 cells it can connect to, and even in quite rural locations the ability to see a handful of cells is the norm. Mobile phone manufactures have spent hundreds of millions of pounds on research and development and on software to optimise the way the modern cell phone connects and interacts with Mobile Networks, ensuring that connectivity is flawless.

Contrast this with the devices designed for specific applications where many have a degree of built-in intelligence, but they rely heavily on being set up correctly for their particular location and traffic profile by an engineer. However the skill set needed to do this is currently in short supply and most field engineers and computer network specialists leave the default setting 'as is'. This in turn degrades the hardware's performance and ultimately the performance of the delivery of the data.

1.3 Cell switching

Cell switching occurs all the time when your device is moving, as you are passed from cell to cell along your journey. It can also occur when your device is static, although less frequently. However, if you are static and connected to a cell that is suffering from network congestion then the cell will ask your device to switch to another cell that is also serving your location.

Due to organic cell switching and operational changes to networks, it is important to note that the network pattern seen at installation of a TEC device can subsequently change. Therefore a good device with a permanent roaming sim is recommended, in order that the system 'self-heals' as time passes.

A word of caution about using a directional antenna to get a better signal. Whilst this will help if your location is served only by a single cell site, if your location is served by multiple cells using a directional antenna will be counterproductive as your device cannot switch to another cell. Installation of a directional antenna will limit your flexibility in the longer term.

C Helpful Advice

Cable length also plays a crucial role when selecting your antenna. Different cables have different properties. For example, imagine using a cable that loses 1db of signal for every metre of cable and an antenna of 5db gain. So you gain 5db at the antenna, the antenna has 5 metres of cable attached to it, so now you are at 0db gain. The connector at the end of the cable also loses 1db, so your effective gain is now -1db! The best "bang for your buck" when a connection is borderline would be spending on a higher gain antenna.

1.4 Multi network SIMs managed roaming

Managed roaming is designed to give you the best connection available in your location through use of a 'Global Roaming SIM'. Managed roaming allows the device to run a site survey when it is first powered up to see what networks are available to it. Networks that have a poor signal or offer low throughput are black-listed and the ones that are left are put in a preferred order (based on signal strength and throughput). When the preferred network has low signal or throughput this is also black-listed and then the next network from the preferred list is selected. Once all networks are black-listed the whole process starts again. This process works well for a fixed location device.

Contrast this with the operation of a simple roaming SIM where the home network applies a set of rules on how the connection is managed, so called 'steered roaming'. For example, consider that you have a SIM from network provider A, and you are network roaming. Your device may select network provider B to connect to. When the authentication request hits A's network they reject it because they want you to use their network where possible, as it costs them less. Your device will usually try this process five times before the provider A's network will allow the authentication request through.

The duration of this process varies by device but is typically ten seconds per retry, which equates to a delay of up to 60 seconds before a connection is made. By this point most applications will be timed out and will reinitiate the process, therefore giving the perception that no connection can be made. A true Global Roaming SIM does not have steered roaming applied to it and will connect to the first network it tries on the assumption that the device has already applied your criteria for the best possible connection at that time.

Note: most non-managed roaming devices switch networks only when the signal of the current network disappears completely, this can cause the device to become 'stranded'. The device has a signal, but as it is marginal it is not strong enough for the device to function. This is another scenario where a strong managed roaming algorithm becomes key.

C Helpful Advice

Be aware of non UK mainland network SIMs. They do roam on to any UK network, but they are given the lowest priority when cells become congested and overuse charges can be very high. Therefore although the ticket price appears very competitive, this is offset by the poor performance and high cost of ownership.
Ensure you have a provider who can offer you 'Permanent Roaming' – very few SIMs are, and they run from consumer roaming agreements that can be limited by regulation to 120days.

1.5 Faulty SIMs

IoT grade SIMs rarely develop faults as they have solid state construction and have no moving parts. They are used to identify the subscriber onto the network. The primary reason they may not work is often the way that they are set up on the network, with the most common problems being listed below.

- **Wrong IP addressing**
- **Duplicate IP addressing**
- **Wrong APN**
- **SIMs being shipped but not activated**
- **SIMs being enabled for WAP not WEB**

ASK YOUR MOBILE SERVICE PROVIDER ABOUT THESE

1.6 Consumer grade SIMs

In 2014 some of the networks reverted to supplying cheaper consumer specification SIMs in some applications. These SIMs have a lower grade EEPROM (Flash memory) on board that means they have a shorter life span, which can be made significantly shorter if the SIM is used as a flash memory in its own right. They also have a smaller cache, again shortening its useful life. The consumer SIM will also have a narrower temperature range thus increasing the chances of failure in some environments and shortening its life span.

Consumer SIM:	**M2M SIM:**
Temperature range of -25°C to +85°C	Temperature range of -40°C to +105°C

1.7 USB Dongles vs Routers

So-called ‘dongles’, which connect via USB, are not designed for permanent installations. Power control is difficult, and there is no connection management, as the user is expected to disconnect the dongle and reconnect it if there is an issue. Also, since the USB port stays live in a power cycle then the standard ‘turn it off and turn it back on again’ process has no effect. The radio module versions are also constantly changing, which can cause incompatibility issues with deployed hardware and large estates of devices become impossible to manage. USB dongles are not designed to manage black holes, and radio performance can be poor. In general, dongles are designed for light domestic/office use and when they are used constantly, they have a Mean Time Between Failure (MTBF) of six to eight months.

With routers the hardware platform is stable and any changes to the radio modules are controlled and tested before they are released. The MTBF is commonly five years. The

manufacturers have connection management to prevent mobile ‘black holes’ (if the device is configured correctly). Hours of engineering time out in the field can be saved by bench testing the manufacturer’s default setting against what is configurable and observing the net result. However, a lack of knowledge about the router’s capabilities is often where projects fail to deliver the performance required by the end user.

C Helpful Advice

When tests are run try to keep them as close to the real thing as possible. For example if your device is sensitive to high latency, do not run the server end on a laptop and use Wi-Fi as the connection, since this will increase the real life latency and give poor results.

Use the hardware and antenna that you are going to deploy with. Do not use a Pay As You Go SIM! Talk to a friendly Mobile Virtual Network Operator (MVNO) that can help you with an M2M SIM for testing.

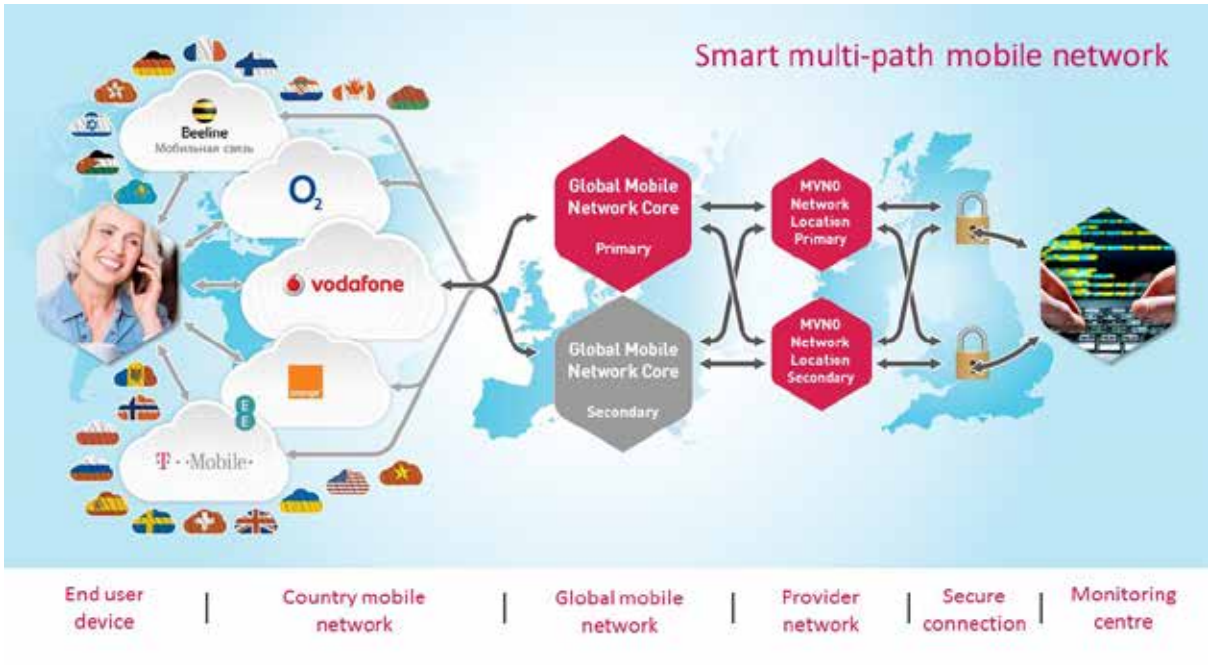
2. Mobile network trustworthiness

2.1 Resilience

Many mobile networks and resellers only offer a single route for the data to flow through and this is a major flaw in most systems. The single data path can become congested with the physical amount of traffic that the network is carrying. This becomes particularly apparent if there is a single Access Point Name (APN) carrying all of the data. This typically manifests itself as a long delay (measured in seconds) and occasional data packet loss. The single path is also susceptible to component failure (router, server and firewall). For many applications where data delivery is not time or mission critical this solution is fine.

But components do fail and systems do go down, leaving disruption lasting hours or in some cases a couple of weeks, due to the lead time on replacement components. There are a few solutions that will claim 99.995% up time, which is certainly eye-opening. However, upon closer inspection this generally only refers to the core network infrastructure and this is achievable with the help of cloud based back up. Check that claimed performance relates to end-to-end availability.

Example below showing multiple data routes using more than one mobile operator



C Helpful Advice

For 99.9995% on-street availability, multipath multi network architecture needs to be employed. This requires not only a network roaming SIM but two connections into the mobile network at GGSN level. This dual connection needs replicating throughout the data pathway until the delivery at the customer's firewall, so there is no single point of failure.

2.2 Cost of failure

If the SIM stops working in your phone the operator will send you a new one, next day, and while you will be inconvenienced, the cost of failure is minimal. However if an IoT SIM used for TECS stops working, recovering the SIM could entail visiting one, two or hundreds of homes of vulnerable people in order to address the issue. This, unfortunately, is a scenario that happens in the real world, all too often.

Frustratingly there may be nothing wrong with the physical SIM. It is set up on the network, and the operator may have changed the profile of the SIM in error. With that in mind it is prudent to check the whole estate every quarter to prevent this. If the resources are not available to carry out this task it should be a consideration when selecting the supplier of the SIMs.

2.3 TECS security and hacking risks

Private Network Fixed IP vs Internet Fixed IP

Do you want to be exposed onto the Internet? These BBC articles highlight the perils of using Public Fixed IP: using public IP addressing, fixed or otherwise, is an invitation to be hacked and it's not if you will be hacked, it's when you will be hacked.

Shodan is a search engine for devices where you can look up all kinds of things you might want to access with malicious intent. It makes the hacking of infrastructure much easier and is not the only one available to everybody.

C Helpful Advice

Using a private Access Point Name (APN) removes all of this risk because from the private APN you can restrict internet access and as all the devices sit on a private network the only way to get to them is through a secure connection from your main office to the operator.

As well as the fact that your system can be hacked freely, you also need to consider the impact on the revenue budget you have for the scheme. You may have bought 10MB because that is what you need, but if anyone who is connected to the internet has the ability to attack your device you lose all control of data consumption, which could potentially cost hundreds or thousands of pounds in additional data costs. You may have a firewall that blocks the traffic when it reaches the SIM's IP, but the fact is that it will have got there by using up your data.

3. Data issues

3.1 Mobile networks as data & voice carriers for TECS

A SIM is just a SIM so why would you need to buy an IoT SIM? In order to answer this question you have to be clear about the expectations of the voice market. A key point to understand is that voice and data have very different expectations and standards. If you have a mobile phone and it doesn't work, most of the time you will be able to borrow somebody else's phone and make that critical call. The cost of failure is likely to be very low. If there is a problem with the phone or the SIM, the network providers are very quick and professional in resolving it, by for example sending out a replacement SIM on a next day basis. You are worth looking after since the income you represent as a phone user is still relatively high and the network providers have a very streamlined and polished way of handling the pattern of issues that do come up. As a result the customer experience is largely good.

In IoT (Internet of Things) and TECS we have a very different story. Here the revenue is much lower at a tenth or less of what a mobile phone consumer is worth. So there are no resources to look after each individual connection with the same high level of intervention that is expected in voice. In IoT there may be no local 'friendly' user and the environment itself may be inaccessible. It is a much more hostile place than a phone is likely to experience. The hardware and firmware will be bespoke so there is not the opportunity to build a profile of likely issues as there is with the relatively limited number of handsets in the market. A call to a customer service desk quickly goes 'off script'. And once you are there you will almost certainly end up being advised to take the SIM out, give it a clean and put it back in again. This will probably work but it is because the SIM is usually behind the battery and by taking the battery out you have performed a hard reset.

That probably does 'fix' the problem. However, it is not a solution; it does not explain why the system failed in the first place. As far as the support call goes, they have done their job, your equipment or service is working again, and they can go on to the next call. This "giving the SIM a clean fix" has had huge implications for the industry. We see then two very different expectations- a voice one where 90 to 96% is good and an IoT and TECSS world that is striving for 99.999 or 5 '9's availability. Keep in mind that 96% means that your system can be out for an hour a day and still be regarded as 'good'. Customers seeking communications services for TECS almost by definition are looking for better.

3.2 Mobile black holes - when data disappears

If you have deployed a mobile solution, you will probably have come across these without actually knowing what they are, or what causes them.

When a device has been connected to a mobile network for a period of time, the network 'sleeps' your radio layer if no data has been transmitted (the period varies depending on the usage of the cell you are connected to). This has no impact on the data layer which stays connected. When you want to send traffic again the radio layer wakes and your session carries on. This is often why the first packet of data sent takes a bit longer than the packets that follow it and this is the radio layer waking up. Occasionally the radio layer does not wake and because you still have an IP layer the software believes it is connected and your packets effectively 'go into a black hole'.

This could be resolved by simply sending a 'ping' or handshake transmission now and again, which increases the data volume used and reboots the device if it fails. More sophisticated solutions monitor a Transmission Control Protocol (TCP) session and recover the session when the TCP connection fails. The strength of the connection is a summation of all the parts in the system and the software controlling it and so requires careful thought from the inception of your scheme onwards.

C Helpful Advice

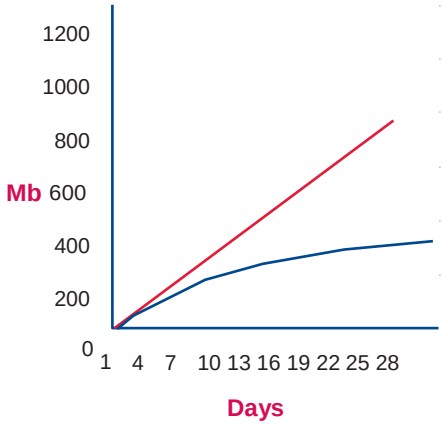
It can be very easy to avoid mobile "black holes" by making sure that your hardware has the ability to manage its own connection. Many of the latest range of modems/ routers have this functionality. (this requires an understanding of the hardware configuration)

3.3 IoT & TECS mobile tariffs

The tariff for your SIM does make a difference. Deals such as unlimited voice, unlimited text and unlimited data, all for a fixed monthly cost, are aimed at the smart phone consumer market. However the operators know that the typical use will only use around 400MB per month and they help you to stay near to that figure by applying a fair use policy.

The policy includes the agreement for the network to choke throughput speeds, filter content and apply involuntary compression. It specifically prohibits over the air updates and streaming. The graph shows the expected usage over a month for a 1GB SIM where the blue line plots the actual throughput for a Mobile Broadband SIM in a TECS installation.

Fair use in practice



Expected usage

Actual usage

- 1GB usage is not linear
- Speed controlled by throttles or by disconnection
- Designed to maintain network availability for all
- Speed attained slows over the month

C Helpful Advice

To ease implementation with internal IT, eek out suppliers with compliance certification that meets or surpasses your corporate Code of Connectivity (CoCo) for example; PCI/DSS (Payment Card Industry / Data Security Standard)

Peer2Peer is also not allowed by the fair use policy. However, most IoT applications use P2P. Your device sends information to the server every hour of every day, which is P2P. All of these filters increase latency by as much as ten times, taking a round trip of 100 milliseconds (ms) and turning it into a second. This level of latency can cause the managing application some difficulties.

An IoT/TECS tariff does not have any of these filters. The typical latency experienced through the IoT platform is less than 80ms from device to end server/ARC with the message passing through the networks servers and infrastructure in sub 10ms. If the user experiences longer

delays than 200ms there is a pinch point either at an Access Point Name (APN) or at a server, which can be found with a series of ping traces.

IoT tariffs are more expensive because the operators know that if you buy a 1GB tariff you are going to use 1GB, and not the 400MB that the average mobile phone user consumes.

3.4 Data aggregation

Data aggregation allows the overall cost of an estate of SIMs to be reduced, as it is very rare for all devices in all locations to use the same amount of data. Typically if 100 devices consume just less than 1MB per month on average, some sites use 2MB and others only 0.5MB. Data aggregation effectively gives 100x1MB SIMs therefore a 100MB pool of data. This prevents paying overage on some SIMs when other SIMs within an estate have spare data.

3.5 Data reservoirs

An issue with the current model of monthly tariffs is that we under buy to minimise cost but run the risk of 'overage' driven by seasonal demand, unforeseen circumstances or technical error. Or we over buy which means that a large of data bought is unused by the end of the month and 'lost'.

The tariff model also means that each tariff, even if aggregated itself, is separate from any other tariff that we may have negotiated. This means it is possible to have overage charges on one tariff despite having large amounts of data unused in another.

The tariff structure creates inefficiencies in that buying small tariffs may result in a cost of £0.20 to £1.00 per megabit of data while large tariffs, though costing more, drive the cost of a megabit down to around £0.01 per MB.

Data reservoirs are large volumes of data, typically multiples of terabytes that change the pricing and give more flexibility.

3.6 4G and Backhaul implications

4G is here for consumers and is now appearing for IoT. If your hardware is 4G ready then you can take advantage of 4G where it is available. The typical latency (time delay) in the 4G network is less than 20ms. With these speeds 4G lends itself for example to

> **C Helpful Advice**
>
> **'Backhaul' and the amount of data through puts are often overlooked when systems are specified.**
>
> **The firewall and server too are often under-specified. This results in a poorly performing system and high ongoing revenue costs, which can terminate the project in the long term. This point also applies to mesh systems as they are often sold as revenue free but do not take into account the possible backhaul costs.**

Telehealth video conferencing and camera control applications.

Most of us think about the speed of our phones without thinking about the network infrastructure in the middle, this is known as 'Backhaul'. All of the carriers talk about super-fast 4G and that you can change your digital life using 4G. In reality we are seeing about five times the speed of traditional 3G. The radio connection is capable of massive speeds but is restricted by the backhaul (i.e. the intermediate links between the core (or backbone) network and the small subnetworks at the 'edge' of the entire hierarchical network) of the supplier. For example 40 users on a 4G cell site will require 1Gbps of backhaul.

When this gets further back in the network and those 40 users become hundreds or thousands of users or devices the backhaul becomes an expensive overhead. Care is needed when choosing suppliers who can support 4G data volumes in their network and can show how they can backhaul it to your server or this too will become a potential point of failure, resulting in high latency and lost packets of data.

3.7 2G/3G/4G longevity

2G – 2025 Sunset

2G Networks have been around the longest, are proven and well utilized. The current switch off or 'sunset' for 2G is scheduled by most Mobile Network Operators (MNOs) for 2025. This has already happened on AT&T the United States. In the UK and Europe, there are a lot of devices still running on 2G and it is, for now, still worth running those networks whilst they are still viable. In the meantime though, coverage on 2G could start to reduce, as the MNO's more favourable licenced frequencies are moved to 3G and 4G to enhance coverage on the more current technologies.

3G – 2020-2022 support ends

3G Networks have a shorter lifespan ahead of them. Most networks are looking at no longer supporting 3G from 2020 with some stretching that to 2022. What 'no longer support' means is open to interpretation, some will wind-down coverage and others will look to switch off completely. Most MNOs now no longer sell a device that doesn't support 4G, in the aim to wash out any 3G only users over the next 2 years. Again you will likely see coverage reductions in the meantime as the favourable frequencies are moved to 4G to further enhance coverage and throughput.

4G – current

4G for now is still current technology and therefore there are no current official notices to withdraw it. As the first iteration of the Long Term Evolution (LTE) Stack, it is likely to remain for some time.

5G – Future

5G is the next generation of LTE network, further enhancing speeds and capacity as well as introducing fundamental changes in the way devices connect to the networks, designed in a more "always on" capacity. Like when 4G was released, although 5G has major advantages over 4G, these benefits, generally, won't have a huge benefit to most Telecare products in the short term, as speeds of transfer for large data isn't a current requirement.

3.8 New Low Power IoT networks – Sigfox, LoRa & Narrowband IoT

New Low Power networks have emerged over the last few years, paving the way to a whole host of connected devices that were never before possible. With battery life up to 10-15years, new monitoring devices from car parking sensors to water meters and sealed GPS trackers are now possible without the need for power. Another added benefit of these technologies is their reach, with up to 30% increase in coverage due to the nature of the technology, these low power technologies are set to cover 'not-spots' all over the country.

Due to the nature of the Low Power technologies, there are restrictions though. The data speeds are slower and intended for small snapshots of information; a GPS location, or a water level, whether a car park space is occupied or not. Some will support voice and larger data packets but with a higher power draw.

As these technologies are still relatively new, there is a 'Betamax vs VHS' question that is still unanswered. You have proprietary technologies such as Sigfox and LoRa that have been out in the field for some time now, but do require you to build the network you want from a base station perspective. This type of set-up may suit a town or city, where the demand is

localised, but coverage outside of that isn't guaranteed. These technologies also run on unlicensed frequencies that are also used by other technologies.

There are also options from the LTE (Long Term Evolution) mobile stack known as Narrowband IoT or NB-IoT. These are based on 4G technology and seem to be favoured by the major Mobile Network Operators. This is as it will likely be only a software upgrade for most mobile sites to support the technology. Vodafone, for example, have launched this in Ireland already in a matter of weeks. This then, is likely to be the mass coverage option, like you would expect from a mobile service today, and without the need to build any networks yourself.

There is no doubt they open up a whole new world of options, but it is worth looking into each technology in great detail before deciding which may be for you.

C Helpful Advice

Where can I get help?

Help to make the task easier help is available from many existing information sources such as:

Web Links:

http://www.bbc.co.uk/news/technology-22524274
http://m.bbc.co.uk/news/technology-28850305
http://www.shodanhq.com/

4. Summary – tips and questions for suppliers

- Ask for core availability statistics for the last three years and on street if available
- Make sure the supplier bills by the byte
- Invest in a good omni-direction antenna
- Ensure it's a global non-steered roaming SIM; preferably with a device roaming algorithm
- Minimise antenna cable length
- Ensure the supplier provides Permanent Roaming
- Be aware of typical SIM network fault reasons – IP addressing / incorrect APN / not activated / WAP not WEB enabled
- Ensure it is a Machine to Machine SIM rather than a Consumer SIM
- Avoid use of USB Dongles for critical or commercial applications
- Test the SIM connection in as real conditions as is possible
- Do not use PAYG SIMs
- Use a SIM that employs Multi-Path Multi-Network architecture
- Use a private APN to restrict the devices that can access the network
- Ensure the hardware has the ability to manage its own connection
- Use suppliers that matches or exceeds corporate Code of Connectivity standards
- Use IoT tariffs to avoid delays in regular data transmission
- Use data aggregation to ensure overuse of one Sim is compensated in underuse of another SIM
- For larger data usage applications; use a supplier that can provide data reservoirs to allow for flexibility around pricing
- Ensure Firewall and Servers are correctly specified to allow the solution to operate at peak performance
- Ensure the supplier has suitable contention ratios within their network to provide high bandwidth media if required

5. Definition of terms

Term	Definition	Description
2G/3G/4G/5G		Different types of mobile phone data systems offering varying speed and connectivity
Analogue phone lines		Traditional phone lines fitted to most homes in the UK, when you dial a number you hear audible tones as buttons are pressed
APN	Access Point Name	The name of a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network, frequently the public Internet. A mobile device making a data connection must be configured with an APN to present to the carrier.
Apps	Applications	Small software programs that run on phones and tablets and perform specific tasks such as providing a location, playing video or music, editing photos etc.
ARC	Alarm Receiving Centre	
ATA	Analogue Telephone Adapter	A plug in adapter that converts an analogue signal to a digital signal
Backhaul		In a hierarchical telecommunications network the backhaul portion of the network comprises the intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network connecting to the end destination.
Cell	An individual mobile transmitter	Each Cell/Transmitter tower for a mobile network, can hold several individual cells, often cells from multiple operators can be housed on the same physical towers, by motorways and in cities for example
Circuit switched		The traditional method of connecting a phone call where a physical path between sender and receiver is established
Cloud applications		Data and computer programmes that operate over the internet rather than being installed on a local desktop computer
Data packets		Individual elements of digital data
db	Decibel	A measure of signal strength / gain for mobile technology.
DTMF	Dual Tone Multi Frequency	A telecommunication signalling system using the voice-frequency band over telephone lines

GGSN	Gateway GPRS Support Node	A major component gateway in the data path of mobile networks.
GPS	Global Positioning System	A network of satellites positioned in earth orbit to determine the location of a GPS enabled device
GSM	Global System for Mobile communications	Mobile phone systems that can transmit data as well as voice
"High-Gain"	Refers to a High Gain Antenna	Designed to increase the signal gain in less covered regions, A high-gain antenna (HGA) for example, could be a directional antenna with a focused, narrow radio-wave beam width.
IMEI	International Mobile Equipment Identity	An electronic serial number that identifies a piece of GSM enabled equipment such as a mobile phone
Internet of Things		A collection of internet connected devices which can connect and communicate with each other and a central management system
IP networks		Internet Protocol is a term used to describe the standard of communication used by internet connected devices
IPsec	Internet Protocol security	A set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner. Also known as IP Security.
Latency		The delay before a transfer of data begins following an instruction for its transfer.
LTE	Long Term Evolution	A term generally used to refer to modern mobile technology from 4G onwards
MNO	Mobile Network Operator	A mobile provider running and managing their own network infrastructure i.e. Vodafone, o2, KPN, Telenor, EE, 3
MTBF	Mean Time Between Failures	MTBF (mean time between failures) is a measure of how reliable a hardware product or component is. For most components, the measure is typically in thousands or even tens of thousands of hours between failures. For example, a hard disk drive may have a mean time between failures of 300,000 hours.

MVNO	Mobile Virtual Network Operator	A specialist mobile provider using a physical network infrastructure managed by an MNO. Some specialise in Consumer i.e. Tesco Mobile, Giff Gaff, Asda Mobile while others specialise in niche markets such as Health i.e. Mobius Networks, CSL, Dualcom.
“Not-Spots”	Areas of no coverage	A phase referring to remote areas of no network coverage from any Mobile Network Operator.
Packet-switched		The braking down of data and voice in to small packets which are sent over an internet connection and reassembled by the receiving system
P2P	"Peer to Peer"	In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server
Roaming		Using an access network other than your “Home” i.e. using the “signal” of o2 UK using a Vodafone SIM.
SIM	Subscriber Identification Module	A smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed.
TCP	Transmission Control Protocol	A suite of communication protocols used to interconnect network devices on the internet.
TDM	Time-division Multiplexing	Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.
VPN	Virtual Private Network	A technology that creates a safe and encrypted connection over a less secure network, such as the internet. *VPN* technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources.