Critical communications
for all professional users

Follow us on @TCCAcritcomms

July 2021

TCCA White Paper

Moving on from Narrowband?

The Top Ten Considerations for Utilities looking to transition from Narrowband to Next-Generation Bearers

Important Note

The opinions and information given in this white paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, TCCA is unable to guarantee the accuracy or completeness of any information contained herein. TCCA, its employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information.

First issued by TCCA's SCADA Smartgrid and IoT Working Group, July 2021.

Introduction

This whitepaper has been produced by TCCA's SCADA, Smartgrid and IoT Working Group. The group's early focus was to promote TETRA as the bearer of choice for SCADA applications. In the meantime, as TETRA has matured and now has a proven track record for SCADA systems, the group has started to look at next generation bearers including LTE and IoT bearers.

The current membership has a strong utility focus but the group is always looking to attract new members from any sector. Please contact Nick Smye, TCCA SCADA WG Chair for more information, at nick.smye@masonadvisory.com

Executive Summary

For mission critical applications, the transition from a traditional narrowband bearer such as TETRA to the next generation of bearers might seem trivial – it is just the same but faster, isn't it? Whilst this is certainly part of the difference, there are more important factors to take into account. In this paper, we have considered what we feel to be the 10 most important factors.

The following items are ranked in order of priority, reflecting a utility sector view for the migration of mission critical services (which for utilities are primarily machine to machine). Other sectors, and particularly more consumer-focused ones, will have different sets of priorities. It also reflects a European perspective in terms of the availability and reliability of infrastructure such as mobile telecoms and the power grid. For other parts of the world, the reality will be different where, for example, bearer and power outages may extend to days.

Top Ten Considerations

1. Risk of Obsolescence

For mission critical organisations such as utilities to embrace a new technology, there needs to be a strong and diverse ecosystem of suppliers that can offer products that are capable of operating in extreme utility environments, and with an appropriate guarantee of longevity. This includes large vendors capable of supporting the infrastructure allied to smaller suppliers focused on niche utility applications. There is a general view that the market will not support the current number of bearer technologies in the marketplace, and that some are likely to fail or become redundant. Utilities and other critical users are therefore reluctant to commit to large-scale deployments of technologies which may not be sustainable over the desired life cycle of the products.

Risk of Obsolescence: Utility infrastructure often has a design life of 50 years or more. Although telecoms equipment is unlikely to have a similar lifecycle, nevertheless, critical users place a premium on the lifecycle of their connectivity technology.

This is particularly relevant where battery devices are deployed in the expectation that the devices can be installed and left to operate for up to ten years without further attention. This is of little benefit if the bearer network is upgraded every three years leaving large numbers of legacy devices orphaned.

A recent example of obsolescence is the phasing out of 3G networks in order to release spectrum for other technologies such as 4G. Thankfully for the utility sector the tens of millions of devices (such as meters) already deployed are primarily using GPRS or LTE and so are unlikely to be affected.

2. Resilience

Resilience is particularly important for mission critical systems and so when looking at the transition to a new system it is necessary to consider not just the bearer but also the underlying network topology and resilience.

Resilience: Critical data services are often required in complex hostile environments where there is limited access for personnel or repair in the case of failures.

A self-provided network can be specifically designed to give the required level of resilience in terms of power, transmission and avoidance (or at least minimisation) of single points of failure. This allows the resilience of the network to be optimised for the application such as providing power backup at all base station and backhaul nodes or minimising the amount of 'daisy chaining' in the backhaul architecture. Daisy chaining can result in multiple sites having service loss as a result of a common backhaul element.

The fundamental purpose of a commercial wireless network is to make a profit and so, up to now, design considerations focus on maximising revenue by providing volume consumer service rather than optimising for mission critical aspects such as security, resilience and performance. For public mobile networks then typically the core would be highly resilient but the backhaul and base stations less so. In dense urban areas there will be a large amount of overlapping coverage which can mitigate for the loss of a single base station but the loss of backhaul or multiple base stations will likely cause a service outage. It remains to be seen whether in the future some mobile network operators will seek to differentiate themselves by offering a more resilient service.

3. Priority and Pre-emption

Whilst this is a key feature of TETRA and other narrowband systems, support for these features varies for the newer bearers. 3GPP-based bearers build upon the priority and pre-emption features introduced with Release 12 of the standard and offer similar features to TETRA. LoRa and Sigfox don't offer priority and pre-emption features.

For mission critical applications priority and pre-emption will be important and especially if a shared public network is being used. For a private network this is still important to allow differentiation of critical traffic (such as smart grid) and non-critical traffic (such as bulk metering data).

4. Coverage

In terms of terrestrial coverage, indoor/basement coverage is a key requirement for applications such as utility metering. Many of the newer bearers can offer a greater range by virtue of a better link budget which can offer an improvement of up to 20 dB. But, of course, coverage also depends upon the density of base stations.

For wide area outdoor coverage, satellite solutions can be attractive. The past few years have seen a lot of activity in Low Earth Orbit (LEO) satellites from players such as OneWeb, Space-X, Amazon and Samsung, to provide a low-latency, high-bandwidth (broadband) internet service to areas that are not well served by commercial mobile networks.

Terrestrial mobile networks will come under increasing commercial pressures to limit rural coverage as systems move higher in frequency and therefore need an increase in base station density even to maintain current coverage requirements (unless 700 MHz and ultimately 600 MHz carry regulatory coverage obligations). If such LEO services are commercially successful then they should be able to serve a diverse and dispersed IoT market.

Coverage: Mission critical services often have to be provided in areas of little commercial interest to public networks.

5. Security

This covers both physical and information security. Physical security is primarily dependent upon the physical implementation of the network, but for information security the level varies with the technology.

At the high end, 3GPP IoT/M2M variants build upon the information security features of LTE/5G which is considered to be relatively secure and includes features

Security: Both physical and electronic security are vital in critical infrastructure. The multiple layers of security employed in physical world must be replicated electronically in the future.

such as network and subscriber authentication and remote key updates.

LoRa information security is based upon IEEE 802.15.4, 128 bit AES and network and application session keys. Sigfox security is limited to a crypto token for device authentication, and anti replay with payload encryption is offered as an option.

But there is a trade-off between security, processing overhead and power consumption. In very general terms, the more secure the solution the more computationally intensive the security algorithms are. So higher levels of security may not be practical either for some low-cost devices with less powerful processors or applications that require a long battery life.

As the number of remote outstations and the functionality of modems increase then it becomes critical to have effective remote management. This includes being able to control what applications can run on the device and patch device vulnerabilities quickly.

6. Wide choice of Bearers

Whilst the obvious choice for a bearer might seem to be the ubiquitous wideband LTE 4G standard, this is optimised for the consumer market where the headline data rates command most attention. But in recent years there has been a huge push to develop technologies optimised for the M2M and IoT market where the need is to support very large numbers of devices, at a low unit cost, with longer range and with the possibility of extended battery operation. This might seem an impossible trade-off but in fact much of this has been achieved and is now well established and this brings exciting new possibilities for mission critical applications.

Wide choice of Bearers: The industrial IoT market is significantly different to the consumer market. Flexibility to deploy large and complex antennas is often possible.

Technologies can be conveniently split into two types, those using licensed spectrum, which offers protection against interference, and those using licence-exempt spectrum, more commonly called ‘unlicensed’ where devices must conform to a standard and spectrum is shared between multiple users and operators and there is no protection against interference.

- Licensed spectrum is primarily used by the 3GPP IoT/M2M variants of 2G-5G technologies, namely LTE-M and NB-IoT. The market is dominated by the existing mobile network operators who have widely adopted these variants as in most cases base stations can be updated with just a software upgrade. These are the most feature-rich bearers and the most attractive for mission critical applications where protection against interference is important.
- In addition to consumer-based technologies such as WiFi, Bluetooth and Zigbee, unlicensed spectrum for industrial applications is dominated by two technologies, LoRa and Sigfox which are optimised for low cost applications with a less rich feature set. Data rates are lower but for cost sensitive applications the simplicity and lower cost of unlicensed spectrum is attractive.

Another thing to consider is whether to use a shared public network or a dedicated private network or some other combination of shared private/public network. The use of a public network will likely offer good coverage in centres of population, but of course guaranteed access to the network in times of stress (using priority and pre-emption) is also paramount for mission critical applications. In the last few years there has been a greater interest from mission critical users such as utilities for private systems, and spectrum regulators are at last beginning to recognise the importance of such systems and award dedicated (licensed) spectrum.

7. Mobile Device Management

The benefit that comes with the ability to install a large number of remote devices at relatively low cost has to be balanced against the overhead of managing these devices. For TETRA, management of the device will likely be done by a technician with a programming device that might be acceptable for say a few 100 devices, but when you start to think about fleets of 1000s of devices then this model just isn’t practical. What is needed is a robust solution that can do this remotely, controlling what applications can be loaded onto the device and performing updates, including scheduling critical security patches etc. For 3GPP variants there are a number of solutions from the commercial world that are eminently suitable and are readily scalable (an example of one such product is VMWare's Workspace One).

Mobile Device Management: Large numbers of devices may need to be configured securely before deployment, and then optimised remotely in the field to match precise and sometimes changing requirements.

8. Device Power

Whilst extended battery operation is not an option with TETRA, many of the newer bearers are optimised for very low power operation, with a typical quoted battery life of up to 10 years. But remember that the laws of physics still apply and to achieve such long lifetimes very low duty cycles and small data payloads are needed. This might be achievable for a metering application where there is weekly reading but for mission critical SCADA applications then more frequent transmissions would likely be required.

Device Power: Mission critical devices may require back-up power in case of loss of mains supply. Batteries in the cover of this pole-mounted telemetry device guarantee continued operation for a minimum of 72 hours after the loss of mains power.

9. Wide range of Modems/Routers

The market for TETRA is a fraction of the consumer/mobile market and as a consequence of the lower volumes, choice is more limited and equipment costs are higher. With the newer bearers, geared to high volume, there is much more choice, from low-cost limited-functionality modems all the way to fully featured enterprise routers. But once again this will also come down to power consumption, and for the very lowest power applications a simpler device could be needed. Today's enterprise routers often include WiFi, firewall and router as well as being available in ruggedized formats from suppliers such as Cradlepoint and Goodmill Systems. Another important difference is that whereas many of today's modems rely upon a serial connection with AT command set, the more modern modems/routers make use of native IP using standard ethernet.

Wide range of Modems/Routers: The types of modems and routers required in critical applications are varied and often need to be ruggedised for harsh operating environments.

10. 5G

These days it is hard to ignore 5G and the features in the specification that are targeted for IoT/telemetry type applications such as Ultra Reliable and Low Latency Communications (e.g. radio latencies of 1-2 ms), network slicing and support for very large densities of devices (e.g. 1,000,000 devices/km^2). But in the short to medium term, 5G coverage will be limited and 5G features are of less interest for mission critical applications moving from a narrowband bearer such as TETRA.

In the longer term some 5G features such as seamless roaming to satellite to reach the most remote areas could be attractive but it remains to be seen how practical this will be for low power applications.

It is also important to remember that 5G is a mobile technology and not a network. So the level of resilience afforded to 5G applications is very much dependent upon the underlying network implementation (power backup, minimised single points of failure etc.) rather than the mobile technology itself.

5G: The ability of 5G to provide Ultra Reliable and Low Latency Communications in high density environments will be a vital requirement if 5G is to be of value in mission critical data applications.

Conclusion

As next generation networks such as 4G, 5G, LoRa and Sigfox become more widespread, there is increasing interest from the utilities sector in the features in the standards that are targeted at IoT telemetry-type applications. New bearers can open up exciting new applications that cannot be served by today's narrowband bearers. In this white paper, TCCA's SCADA, Smartgrid and IoT Working Group has shared its view of the top ten considerations for utilities looking to transition from narrowband to next-generation bearers for mission critical applications. Different sectors and regions of the world will likely have different priorities. The Group hopes that the discussions around these topics will help organisations that are planning to migrate their machine-to-machine (M2M) communications to a new bearer or bearers.