March 2018

Emerging Wireless Bearers for Mission Critical SCADA

Produced by TCCA's SCADA, Smart Grid and Telemetry Working Group

Important Note

The opinions and information given by TCCA 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.

Issued by TCCA - First published March 2018

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TCCA Limited is a company incorporated under the Companies Act in England and Wales, company number 04155039.
Registered office: The Grainger Suite, Dobson House, Regent Centre, Gosforth, Newcastle NE3 3PF, UK

Contents

Introduction	2
Mission Critical SCADA	3
Use of commercial mobile networks for Mission Critical SCADA	3
Current wireless bearers	4
Emerging bearers	4
3GPP 2G/3G/4G based Solutions	5
Licence Exempt Low Power Wide Area (LPWA) Technologies	5
5G	6
Comparison of Bearers	7
Comparison summary	8
Annex 1 – Technical Summary of Emerging Wireless Bearers	9

Introduction

This whitepaper has been produced by the TCCA SCADA Group[1] and looks at emerging wireless bearers for mission critical (MC) Supervisory Control and Data Acquisition (SCADA) applications. Within this paper the term SCADA is used quite generally and it is intended to include traditional telemetry and telecontrol applications. Typical SCADA applications include controlling and monitoring the flow of water, electricity, etc. through to civil defence warning systems.

MC SCADA systems require rugged, reliable and cost effective communications and a number of different wireless technologies are used successfully to meet this requirement including TETRA and point to multipoint VHF and UHF systems.

Over the past few years there have been major developments in mobile broadband technologies (such as 3G and 4G) and these have enabled the massive growth in mobile data, smart phones and applications. At the same time the use of the internet and associated cloud based services has expanded dramatically.

This in turn has led to the development of new communication bearers to support the vast number of anticipated IoT devices, including 4G, NB-IoT and future 5G systems, as well as low power wide area technologies based on licence-exempt spectrum such as LoRa and Sigfox.

This white paper explores these emerging wireless communication technologies as potential bearers for MC SCADA and compares and contrasts them with traditional wireless bearers such as TETRA.

Further technical details of current and emerging bearers are given in a TCCA SCADA Working Group Technical Primer document[2] .

[1] For further information on the TCCA SCADA, Smart Grid and Telemetry Working Group please see: https://tcca.info/tetra/scada/

[2] Technical Primer - Current and Emerging SCADA Wireless Bearers, available from https://tcca.info/tetra/scada/

1.1 Mission Critical SCADA

MC SCADA is considered to be a SCADA system that supports services that are critical to the operation of a business, and where danger to life may occur if the service failed. Some examples are given in the following table

Sector	Mission Critical SCADA Application
Electricity Distribution	Network automation, telecontrol of medium voltage network, smart grid
Water	River level monitoring
Oil and Gas	Oil reservoir management, gas condensate pipeline, gas distribution, cathodic protection
Civil Defence	Emergency warning sirens for flooding or civilian emergency

In order to further contrast and compare future wireless technologies in this white paper some typical requirements for a generic MC SCADA application are given below:

- High level of security (MC SCADA is often controlling critical national infrastructure)
- Guaranteed Quality of Service (QoS)
- Highly resilience architecture (power backup, use of licensed spectrum etc.)
- Speed – relatively slow speeds, few kbps.
- Latency: typically 1 – 30 seconds (very dependent upon application)
- Data volumes: typically 1kb per transaction
- Coverage: depends upon application. Links typically up to a 30 km radius around the base station, but in exceptions, longer links may be used

1.2 Use of commercial mobile networks for Mission Critical SCADA

Traditionally wireless MC SCADA used a self-provided network that was 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.

Conversely commercial mobile networks are designed to maximising revenue. Therefore any use of a commercial mobile network for MC SCADA needs to consider carefully the inherent resilience of the host network.

In some cases multiple bearers may be used to enhance resilience, with the bearers using dissimilar technologies. An example of this could be a commercial network and a satellite backup.

Where a public safety user shares a commercial LTE network then priority and pre-emption (included in 3GPP Release 12) will be needed to be able to offer guaranteed quality of service for public safety users. Also it is likely that network hardening will be put in place such as power backup and resilient transmission will be introduced to meet public safety requirements.

Of particular interest to MC SCADA applications considered in this whitepaper are the emerging public safety projects using LTE such as FirstNet in the USA, ESN in the UK and SafeNet in South Korea. These may require enhanced levels of resilience compared to normal commercial networks which could also be beneficial for the support of MC SCADA users.

2. Current Wireless Bearers

Wireless bearers that are currently used for SCADA include the following:

Bearer	Type	Typical Range	Description
TETRA	Mobile	Long	Mobile technology developed for public safety available in various bands between 380 MHz and 900 MHz
Point to multipoint VHF/UHF	Fixed	Very Long	Usually planned around a base station which continuously polls fixed points on the network
Satellite	Fixed	Very Long	Usually based on a fixed satellite network but some applications use the mobile satellite networks to overcome the need to have a dish pointing very accurately to a single point in the sky
GPRS	Mobile	Medium	Mature 2.5G technology for public mobile networks
DMR	Mobile	Long	Digital Mobile Radio standard for business radio users. DMR has more flexibility in use of spectrum than TETRA, and is available in VHF frequencies which are ideal for wide area coverage
CDMA 450	Mobile	Long	Mature 3G technology for public mobile networks. Use of 450MHz gives good coverage over wide areas
WiMax	Fixed	Long	Wireless broadband OFDMA standard developed for wireless metropolitan area networks
Wi-Fi	Fixed	Short	Ubiquitous short range technology used in billions of devices
Wi-SUN	Fixed	Medium	Developed to address the needs of Smart Utility Networks, which require low power, medium range, peer-to-peer Field Area Networks
Zigbee		Short	Short range wireless mesh networking technology based upon the IEE 802.15.4 standard which is optimised for battery operation

These continue to serve SCADA schemes and they are being further developed to compete against the emerging bearers.

3. Emerging Bearers

3.1 Background

The explosion of the IoT is driving the need for cost effective low power wide area (LPWA) communications and volumes of IoT devices are predicted to reach many billions. Key enablers for IoT wireless communication bearers include[3]:

- A very low unit cost to make the business case viable (this in turn requires a simple radio interface/protocol in order to simplify the chipset)
- Devices only need low data rates and can tolerate increased latency
- Support for very high cell density of devices
- Battery operation with typically a 10 year battery life
- Needs to work 'out of the box' as it is impractical to individually provision large numbers of devices
- Improved coverage (e.g. 20 dB better than that achieved by current 3GPP technologies)

These requirements are challenging and have driven the innovative technical solutions which are described further in this section.

[3] 3GPP TR 45.820 Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT) (Release 13)

3.2 3GPP 2G/3G/4G based Solutions

Standard LTE offers very high data rates and low latency but doesn't support extended battery operation and/or the range enhancements that are needed for IoT.

3GPP have introduced three variants to address IoT applications which can all be implemented by a software upgrade. These are summarised as follows:

Variant	Description	Target Market
EC-GSM	EC-GSM brings IoT targeted improvements for the lower radio layers of GSM/GPRS/EDGE networks.	Operators that don't have LTE
LTE-M	LTE-M is based upon the standard LTE wide band radio interface but includes IoT enhancements for battery life and coverage.	Existing LTE Operators and private networks
NB-IoT	NB-IoT is a new narrow band radio interface for LTE. It is flexible to deploy from a spectrum point of view as it is designed to operate in a 200kHz carrier re-farmed from GSM or using shared spectrum in an existing LTE network, thus requiring no additional deployment of antennas, radio or other hardware. It also offers the best coverage.	Existing LTE Operators

All these variants have a similarly high level of security as the basic 4G service. Data rates are lower than for basic 4G, but still more than adequate for MC SCADA. They offer slightly different levels of coverage but all are better than the basic 4G service (See Annex 1).

3.3 Licence Exempt Low Power Wide Area (LPWA) Technologies

This section focuses on two of the emerging low power wide area licence exempt technologies. Fierce competition is expected from the 3GPP based operators and the market is not expected to be big enough to support all players in the longer term. There is therefore a risk of committing to a technology that may become obsolete.

Both use unlicensed spectrum (e.g. 868 MHz in EU) which offers no regulatory protection from interference, and imposes some limits on power and duty cycles that can be used to protect other users (< 10%).

3.3.1 LoRa

LoRa (short for Long Range) is an open standard specification which is maintained by the LoRa Alliance. LoRa Alliance members develop the higher level protocols that define device interoperability and data transfer between devices and the user host server.

LoRa uses an adaptive rate spread spectrum technique developed by Semtech, a French semiconductor company. Three different types of devices are supported depending upon the required downlink latency and power consumption.

LoRa has a flexible architecture and allows the creation of different sized networks, from on-site coverage, to city to national. A number of operators offer LoRa services but private LoRa networks are also possible. A private LoRa nework could be quite attractive for remote areas where there is no coverage from commercial networks.

LoRa uses spread spectrum technology and an adaptive data rate that allows the data rate to be dynamically traded for coverage at cell edges.

Security is based upon IEEE 802.15.4, 128 bit AES and network and application session keys.

The LoRa Alliance states[4] that there are 57 public LoRa operators as of November 2017 operating in more than 100 countries.

3.3.2 Sigfox

Sigfox operates a proprietary 'device to cloud' wireless network through operator partners in different countries that deploy and operate a local radio access network. The core network is essentially cloud based hosted in secured data centres. Sigfox claims that the network offers the lowest energy consumption from device to cloud.

Sigfox is positioned as an ultra low cost service. It uses an ultra narrow band technology which offers a very low data rate (100 bps) and very low cost hardware but there is a limitation on the number of messages per day that can be sent or received (140 x 12 byte messages/day on the uplink and 4 x 8 byte messages/day on the downlink).

Security is limited to a crypto token for authentication and anti replay. Payload encryption is offered as an option.

It is claimed[5] that there is coverage in 36 countries as of November 2017 with nationwide coverage in 17 countries.

3.4 5G

5G is the next (or 5th) mobile network generation, following GSM (2G) 3G and 4G/IMT. It will be characterised by higher data rates, and higher capacity, reduced latency and improved coverage and spectral efficiency. It will have a new radio access network and support large numbers of simultaneous connections, specifically the IoT and Machine to Machine (M2M).

While there is no global standard at the moment, the standards bodies have developed requirements, and mobile equipment manufacturers are developing and trialling 5G technology components.

Whilst there has been a lot of interest in 5G, some[6] have questioned whether given the maturity and performance of 4G there is really a market need for 5G technology. For mobile operators a major investment will be required for 5G, which will require new equipment and significant spending on radio spectrum licences.

So whilst 5G may bring incremental benefits for MC IoT, such as low latency and highly reliable services, it is still too early to say how this will develop.

[4] https://www.lora-alliance.org/
[5] https://www.sigfox.com/en/sigfox-story
[6] See 'The 5G Myth', William Web ISBN 9781 540465818, 2016

4. Comparison of Bearers

In this section emerging bearers are compared for two different MC SCADA scenarios, firstly using a standard commercial wireless network and secondly for an enhanced commercial or private wireless network.

In the following tables the different wireless technologies are listed in the columns and key metrics are listed in the rows. LTE Release 8 (LTE R8) is listed in the first column to represent 'standard' LTE, followed by the emerging bearers and finally TETRA to give a comparison to current TETRA MC SCADA.

4.1 Use of Standard Commercial Network

The following table compares the various bearers for the considered MC SCADA application. The underlying assumption is that the commercial wireless network operator has not implemented quality of service features or increased resilience above the normal level for a commercial network.

Metric	LTE R8	NB-IoT	LTE-M	EC-GSM	LoRa	SigFox	TETRA[1]
Battery Life	✗	✓	✓	✓	✓	✓	✗
#devices	✗	✓	✓	✓	✓	✓	✗
Security	✓	✓	✓	✓	?	✗	✓
Throughput	✓	✓	✓	✓	Cell Edge ?	✗	✓
QoS	?	?	?	?	✗	✗	✓
Resilience	?	?	?	?	✗	✗	✓
Spectrum	✓	✓	✓	✓	?	?	✓
Latency	✓	✓	✓	✓	?	✗	✓
Coverage	✗	✓	✓	✓	✓	✓	✓
Cost	✗	✓	✓	✓	✓✓	✓✓	?
Longevity	✓	✓	✓	[?]	?	?	[?]

NOTE1: For the purposes of this comparison this can be either a TETRA1 carrier or a TEDS carrier

Table 1 – Comparison of Standard Mobile Network and other IoT Bearers

4.2 Use of Enhanced or Private Wireless network

In the following table the assumption is made that either a private network has been rolled out or a commercial wireless network operator **has** implemented quality of service (QoS) **and** increased resilience (maybe because they are providing service to a public safety organisation).

Metric	LTE R8	NB-IoT	LTE-M	EC-GSM	LoRa	SigFox	TETRA[1]
Battery Life	✗	✓	✓	✓	✓	✓	✗
#devices	✗	✓	✓	✓	✓	✓	✗
Security	✓	✓	✓	✓	?	✗	✓✓
Throughput	✓	✓	✓	✓	Cell Edge ?	✗	✓
QoS	?	✓	✓	✓	✗	✗	✓
Resilience	?	✓	✓	✓	?	✗	✓
Spectrum	✓	✓	✓	✓	?	?	✓
Latency	✓	✓	✓	✓	?	✗	✓
Coverage	✗	✓	✓	✓	✓	✓	✓
Cost	✗	?	?	?	✓✓	✓✓	?
Longevity	✓	✓	✓	[?]	?	?	[?]

NOTE1: For the purposes of this comparison this can be either a TETRA1 carrier or a TEDS carrier

Table 2 - Comparison of Enhanced Mobile Network and other IoT Bearers

4.3 Comparison Summary

The preceding tables have compared the suitability of different wireless bearers for the specific MC SCADA requirements described in Section 1.1

For a standard commercial wireless network, none of the emerging bearers is considered suitable for the generic MC SCADA application described in Section 1.1, most commonly because of a lack of QoS/resilience. Note that for the 3GPP bearers at least, this is more of a network implementation issue rather than any limitation in the standards. For LoRa and Sigfox the use of unlicensed spectrum is also considered as a limiting factor.

For an enhanced commercial or private wireless network, the 3GPP based bearers *could* be suitable for MC SCADA but there is a question about the cost of implementing QoS/resilience to the required level. For LoRa whilst a resilience private network could be built, the main issue is the lack of QoS and the use of unlicensed spectrum. It isn't possible to build a private Sigfox network and the very low throughput and weaker security of the standard Sigfox offering rules this out for mission critical use.

Annex 1 - Technical Summary of Emerging Wireless Bearers

A technical summary of the bearers considered in this white paper is given below.

	Basic LTE (R8)	EC-GSM	LTE-M	NB-IoT	LoRa	Sigfox	TETRA1	TETRA TEDS[7]
Coverage Metric (Relative to basic LTE figure 144dB)[8]	0 dB	+20 dB to +10dB	+15dB to +12 dB	+20 dB	≈+13 to -24 dB (depending upon data rate)	≈+16	=+3dB (400 MHz)	=+5dB (4QAM 400 MHz)
Bandwidth	1.4-20 MHz	200 KHz	1.08 MHz	180 KHz	125/250 KHz	100 Hz	25 KHz	50 KHz
Peak Data Rate UL DL	10 Mbps 5 Mbps	70—240 Kbps 70—240 Kbps	1 Mbps 1 Mbps	50 Kbps 50/20 Kbps	50 Kbps 50 Kbps	140 messages/day 4 messages/day	Upto 3 Kbps Upto 3 Kbps	Upto 80 kbps Upto 80 kbps
Target Battery Life (2 AA cells)	Days	10 yrs (traffic dependent)			10 yrs (type A/B) N/A (type C)	10+ yrs	Days	Days
Latency	Low	Low			High (Type A) Med (Type B) Low (Type C)	High	Low	Low
Security	High	High			128 bit AES	Crypto token, no payload encryption	Med to High	Med to High
Priority & Pre-emption	yes	Yes			No	No	Yes	Yes

[7] TEDS has a number of different bandwidths and modulation levels. For the purpose of this comparison a 50 KHz bandwidth is assumed

[8] This is gives an indication of the level of coverage, the higher the number the better the coverage (also depends upon the frequency band)