

September 2019

Emerging IoT Bearers for Non-Mission Critical SCADA

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.

First published September 2019 by TCCA's SCADA, Smart Grid and Telemetry Working Group.

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

Emerging IoT Bearers for Non-Mission Critical SCADA

1. Introduction

This white paper has been produced by TCCA's SCADA Group[1] and it looks at emerging Internet of Things (IoT) wireless bearers for non-mission critical (non-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 utilities such as water and electricity through to automated transit systems.

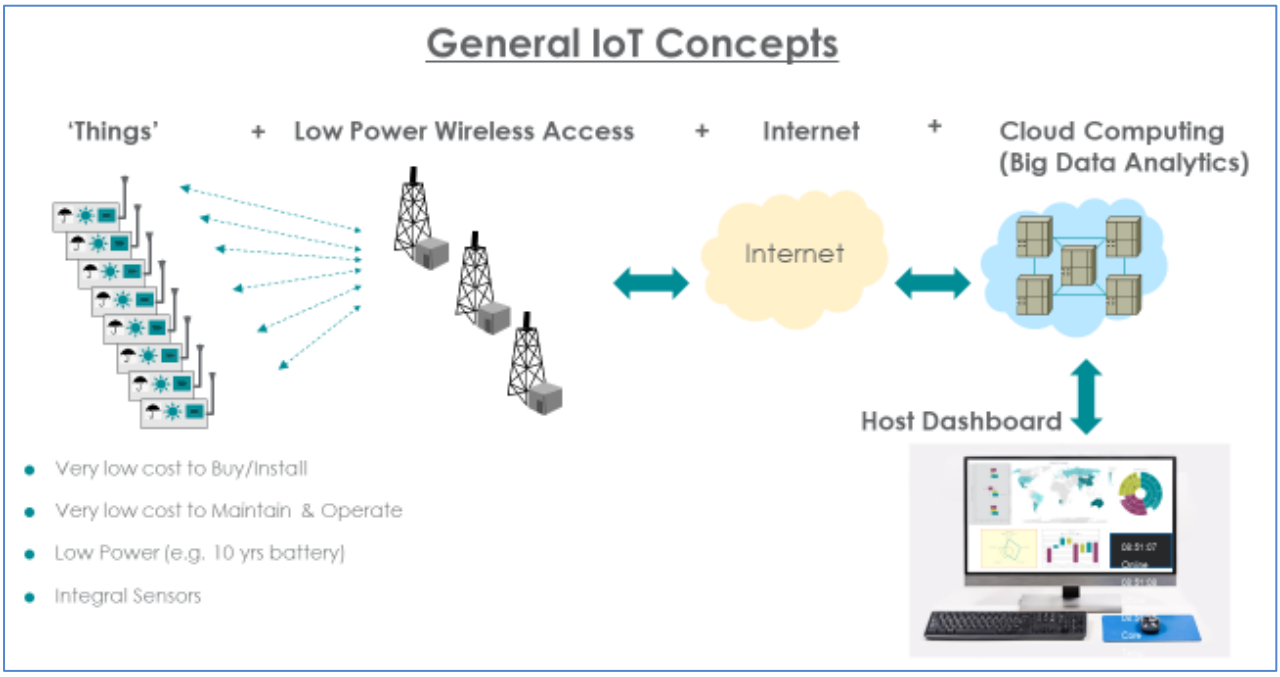
Over the past few years there have been major developments in mobile broadband technologies and these have enabled the massive growth in mobile data, smartphones and applications. At the same time the use of the Internet and associated cloud based services has expanded dramatically.

Most recently there has been the rise of low power wireless technologies to support the anticipated growth of Internet of Things (IoT) devices. These can be split into technologies using licensed spectrum such as 4G, NB-IoT and future 5G systems, as well as technologies based on licence-exempt spectrum such as LoRa and Sigfox.

This white paper explores these emerging wireless communication technologies as potential bearers for non-MC SCADA.

2. What is IoT?

The Internet of Things (IoT) is quite a broad term which means different things to different people. But the general concept is that a very large number of 'things' (devices that include sensors) are connected via wireless links and the Internet to centralised applications.



[1] For further information on the TCCA SCADA, Smart Grid and Telemetry Working Group please see:

https://tcca.info/tetra/scada/

Volumes of IoT devices are forecast to continue to grow fast, with predictions of between 20 - 30[2] billion devices by 2020.

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 wideband 3GPP bearers)

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

3. Non-MC SCADA Applications

The IoT is opening up potentially new groups of non-MC SCADA applications that would not have been feasible with traditional solutions. These can offer considerable business benefits.

Some examples of potential non-MC applications are:

Application	**Characteristics/Benefits**
Electricity Fault Passage Indicators	Aids fault detection and restoration of electricity supply
400v LV connection boxes, branches etc.	Parts of the distribution networks are controlled by switching points called link boxes. Link box safety has become a high profile issue following a small number of incidents involving explosions under pavements
Smart Manhole Cover	Detects: • opening, entry and obstruction • flooding, smoke, fire and gas • movement – theft
Wooden Pole Inertial Monitoring System	Detects deterioration of the structural integrity of wooden poles well before they fail by detecting movement and static lean/tilt
Metering	Revenue, network & demand management
"Internet of Bins"	Smart Bin. Solar powered rubbish compactor that alerts when it needs emptying. Holds 8 x more rubbish and reduces collection frequency by 80%
Smart street lighting	Can also host weather, pollution, car and people counting, gunshot detection etc.

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

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

Monitoring the condition of public infrastructures for safety	Many bridges or tunnels are now ageing. e.g. AT&T is monitoring bridges in New York
Smart Parking	Identify empty parking places and offer to end users via apps to speed up traffic flow and reduce fuel consumption

4. Emerging Bearers

4.1 3GPP 2G/3G/4G based Solutions (licensed spectrum)

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

3GPP has introduced three variants to address IoT applications that 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 or private LTE networks
NB-IoT	NB-IoT is a new narrowband 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, in part because it has the narrowest carrier bandwidth.	Existing LTE Operators or private LTE networks

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 non-MC SCADA. They offer slightly different levels of coverage but all are better than the basic 4G service (See Annex 1).

4.2 Licence Exempt Low Power Wide Area (LPWA) Technologies

This section focusses on two of the emerging low power wide area licence exempt technologies. Fierce competition is expected from the mobile network 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, whilst being free to use, offers no regulatory protection from interference, and imposes some limits on power and duty cycles that can be used to protect other users (< 1%).

4.2.1 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 and 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 state[4] that there are 96 LoRa operators (as of November 2018) operating in more than 100 countries.

See Annex 1 for further technical details.

4.2.2 Sigfox

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

Sigfox is positioned as an ultra low cost service. It uses an ultra narrowband 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 stated[5] that there is Sigfox coverage in 53 countries and regions as of November 2018.

See Annex 1 for further technical details.

4.3 5G

5G is the next (or 5th) mobile network generation, following GSM (2G) 3G and 4G/LTE/IMT. It is 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 Internet of Things and Machine to Machine.

The 5G standards will include support for critical communications, in terms of high performance, ultra-reliable and low latency communications for industrial IoT and mission critical applications. It also brings support for even higher densities of IoT. Whilst LTE Release 13 was intended to support more than 50,000 devices per sector, 5G is intended to supported 'Massive IoT' with more than one million devices /km^2.

[4] https://www.lora-alliance.org/
[5] https://www.sigfox.com/en/sigfox-story

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.

It is believed that in the short to medium term, 4G/unlicensed IoT networks have sufficient capacity and so for this non-MC whitepaper, 5G isn't considered any further at this stage.

5. Comparison of Bearers

For comparison purposes, the following metrics for a typical non-MC SCADA type application are assumed:

Metric	Minimum Requirement	Notes
Battery Life	Target of at least 10 years	This minimises installation and operational costs. Battery life is very dependent upon the size and frequency of data transmissions. For traditional utility SCADA type applications with frequent polling, battery only operation poses a challenge.
Device Density	5,000	Number of devices that can be supported in a given area. Based upon a subset of 3GPP Release13 requirements of 50,000 devices per sector
Security[7]	Depends upon application	The security agenda for anything which either controls utility assets or collects data which will significantly impact control algorithms is becoming a major concern since they have to be able to withstand attacks initiated by sovereign states.
Throughput	140 messages per day	Depends upon application, assumed for the majority of applications 140 messages per day is sufficient
QoS	Not required	
Resilience	Best effort	
Spectrum	Unlicensed spectrum	
Latency	10s of seconds	
Coverage	At least 15db better than GPRS	To allow for coverage into difficult locations such as basements

[6] See 'The 5G Myth', William Webb ISBN 9781 540465818, 2016

[7] See LWPA Security Whitepaper from Franklin Heath Ltd for a detailed analysis of the security of LPWA, https://franklinheath.co.uk/2017/05/02/lpwan-security/#more-1595

Cost	As low as possible	
Longevity	As long as possible	Fierce competition is expected from the 3GPP based operators for whom IoT can be implemented with a software upgrade. This gives them a considerable advantage over new entrants who have to build a completely new network. For this reason it is questionable whether the market can support all LPWA players in the longer term

Table 1 – Typical Metrics for non-MC SCADA Applications

The following table maps the metrics to the IoT bearers:

Metric	LTE R8	NB-IoT	LTE-M	EC-GSM	LoRa	SigFox
Battery Life	✗	✓	✓	✓	✓	✓
Device Density	✗	✓✓	✓	✓	✓	✓
Security	✓✓	✓✓	✓✓	✓✓	✓	?
Throughput	✓✓	✓	✓✓	✓	✓	?
QoS	N/A	N/A	N/A	N/A	N/A	N/A
Resilience	✓	✓	✓	✓	✓	✓
Spectrum	✓✓	✓✓	✓✓	✓✓	✓	✓
Latency	✓	✓	✓	✓	✓	✓
Coverage	✗	✓	✓	✓	✓	✓
Cost	✗	✓	✓	✓	✓	✓✓
Longevity	✓	✓	✓	?[1]	?	?

NOTE1: Longevity is more likely determined by life of the GSM network rather than EC-GSM as such

Table 2 -Comparison of IoT Bearers

Symbol	Meaning
✓✓	Exceeds metric
✓	Meets metric
?	May meet metric for some applications
✗	Doesn't meet metric

It can be seen that, for the generic non-MC application, all of the considered IoT bearers are potentially suitable, the only caveat being that for the Sigfox bearer, where the suitability of the security mechanisms will be very much application dependent.

3GPP based mobile networks are relatively mature and it is safe to assume that IoT bearers will continue to be supported for a long time. For the unlicensed bearers, it is not clear at the moment whether the market can support both LoRa and Sigfox technologies in the longer term.

6. Summary

This whitepaper has considered a number of emerging wireless bearers that have been specifically developed for IoT applications. Some of these use licensed spectrum (3GPP technologies) and the others use licence-exempt spectrum (LoRa and Sigfox).

The technical parameters of the bearers vary widely, with uplink bandwidths between 1Mbps and 140 messages per second and radio carrier bandwidths between 1.08 MHz and 100 Hz. But all offer long range, lower power and a level of security.

In terms of longevity there is a question as to whether all of the current IoT bearers/operators will survive in the longer term given the likely fierce competition from incumbent mobile network operators and the price criticality of the IoT service for applications with very large numbers of connected ‘things’.

For the generic non-MC applications considered, any of the IoT based bearers would be suitable, except for applications needing higher levels of security.

Annex 1 - Technical Summary of Emerging Wireless Bearers

	Basic LTE (R8)	EC-GSM	LTE-M	NB-IoT	LoRa	Sigfox	TETRA
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)
Bandwidth	1.4-20 MHz	200 kHz	1.08 MHz	180 kHz	125/250 kHz	100 Hz	25 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
Target Battery Life (2 AA cells)	Days	10 yrs (traffic dependent)			10 yrs (type A/B) N/A (type C)	10+ yrs	Days
Latency	Low	Low			High (Type A) Med (Type B) Low (Type C)	High	Low
Security	High	High			128 bit AES	Crypto token, no payload encryption	Med to High
Priority & Pre-emption	yes	Yes			No	No	Yes

[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)