masonadvisory

Critical Communications World 2017

Mission critical SCADA - how do future wireless technologies shape up?

16 May 2017 | Nick Smye

What are SCADA, Telemetry and Telecontrol?

- **SCADA** stands for **Supervisory Control and Data Acquisition**
- **Telemetry**: the remote measurement and reporting of information, from remote sensors, meters etc.
- **Telecontrol**: the remote control of equipment such as power switches and breakers, including load control/ load shedding, valves and actuators. Telecontrol systems normally include telemetry functions in order to report back the current status
- **SCADA** is used generally in this presentation and includes smart grid, telemetry and telecontrol applications

What is Mission Critical SCADA?

- SCADA that supports services that are critical to the operation of a business. Examples are:
  - Electricity Distribution - automation, telecontrol MV network, smart grid
  - Water - river level monitoring
  - Oil and Gas – oil reservoir management, gas condensate pipeline, gas distribution, cathodic protection
  - Emergency warning sirens for flooding or civilian emergency

Typical Electricity Distribution Network Operator Wireless Requirements

Application	Latency	Data volume	Est. #units by 2020	Description	
Protection	5–10 ms	1 KB	215	Unit, distance, blocking signals	✗
SCADA Subst. > 100Kv	100 ms	1 KB		Monitoring and control of devices at substations and generation	✗
SCADA Distrib. & Automation	1s	1 KB	25 000	Distr. Substations below 100KV and Distribution Automation (DA)	✓
SCADA Smart Grid Hub	1s	1 KB	5000	Monitoring and control of local distribution points	?
SCADA Smart Grid Concentrator	10s	1 KB	50 000	Allows collection of local demand and supply data	✓
SCADA data recorder	1 minute	1 MB	2500	Temperature, windspeed etc.	✓
Metering	1–30 min	1 KB - 100 KB	Up to 5 million	Revenue, network & demand management (bulk data 24 hours)	✗
Home display	5 min	1 KB	5 million	Planned outage and emergency restoration times (predicted 5 million units in/2020)	✗
Home control	10 min	1 KB	250 000	Allows supplier to remote control load, thermostats etc.	✗

Note: Figures are for a typical European distribution network operator

Source: EUTC Member Survey http://www.eutc.org

Typical Mission Critical Requirements

- High level of security
- Guaranteed Quality of Service (QoS)
- Highly resilience architecture (power backup, use of licensed spectrum etc.)
- Speed – relatively slow speeds, few kbps .
- Latency 1 – 30 seconds (dependant upon application)
- Data volumes – typically 1kb per transaction
- Coverage – depends upon application
- Unit volumes – 10s to 10,000s
- Resilient power (e.g. battery backup)
- [Above is typical of today's TETRA MC application]

Background to IoT and LPWA

- Explosion of Internet of Things (IoT) is driving the need for cost effective low power wide area (LPWA) communications
- Volumes of IoT devices are predicted to grow to many billions of devices:
  - The unit cost of an LPWA solution needs to be very low
  - Low data rates and tolerate increased latency
  - Very high cell density
  - Typically 10 year battery life and work out of the box
- Until recently, 3GPP was focussed on 3G/4G higher data speeds for smartphones (and little concern for battery life) but there has been a huge standardisation push over the last two years.
- Many other low power wide area wireless technologies, this presentation has focussed on two of the front runners LoRa and SigFox

Future Technologies -3GPP Based

- LTE based solutions[1]
  - *basic LTE*
  - LTE-M, wide band radio interface but lower power
  - NB-IoT, new narrow band radio interface
- GSM based
  - EC-GSM, IoT support for GSM/EDGE networks

R13 Requirements [2]

- At least 20dB improvement over GPRS
- Min battery life 10 years
- Massive number of devices (e.g. 40 devices per household, 52,547 per site/sector)
- Reduced device complexity
- Latency can be relaxed

SOURCES

[1]: http://www.3gpp.org/images/presentations/2016_11_3gpp_Standards_for_IoT.pdf

[2]: 3GPP Technical Report TR 45.820

Some 3GPP IoT deployments

- NB-IoT
  - Vodafone – NB IoT, Germany, Ireland, the Netherlands and Spain
  - Deutsche Telecom – commercial launch in Germany Q2 2017. Netherlands to be rolled out by end of 2017
  - Singtel – trials
- LTE-M
  - Verizon - USA, LTE-M1 network launch early in 2017
  - Orange – LTE-M roll-out will begin in Belgium and Spain in 2017, with the rest of Orange's European footprint set to follow
- EC-GSM-IoT
  - Orange – trial in Paris 2016

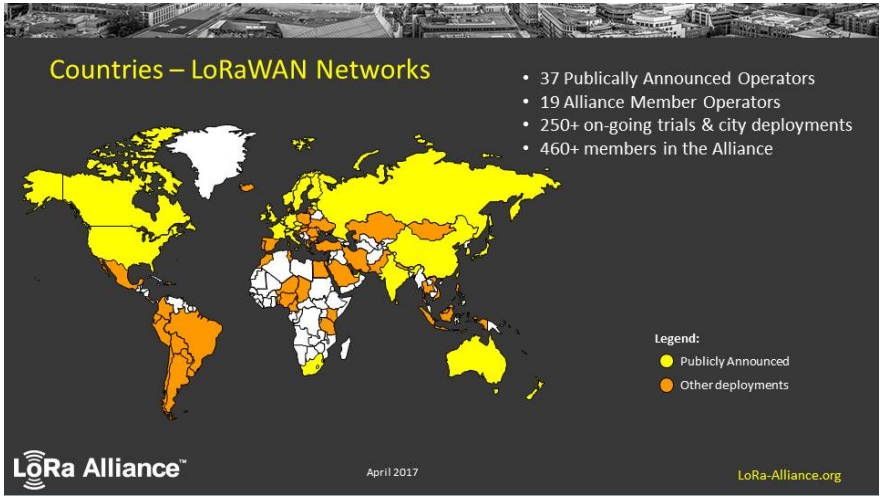
Future Technologies -3GPP Based

	Basic LTE (R8)	NB-IoT	LTE-M	EC-GSM
UE Category	1	NB1	M1	
MCL	144 dB	164 dB	156 dB	164/154dB
Bandwidth	1.4-20 MHz	180 KHz	1.08 MHz	200 KHz
Peak Data Rate UL DL	 10 Mbps 5 Mbps	 50 Kbps 50/20 Kbps	 1 Mbps 1 Mbps	 70—240 Kbps 70—240 Kbps
Power Class	23 dBm	23 dBm	23dBm,20dBm	33dBm/23dBm
Target Battery Life, 2 AA cells	Days	10 yrs (Traffic dependent)	10 yrs (Traffic dependent)	10 yrs (Traffic dependent)
Security	High	As LTE	As LTE	As LTE

SOURCE: http://www.3gpp.org/images/presentations/2016_11_3gpp_Standards_for_IoT.pdf

LoRa

- Open standard specification managed by LoRa Alliance (Semtech chips)
- Unlicensed spectrum (e.g. 868 MHz in EU) – limited power and duty cycle < 10%
- Uses spread spectrum and simple protocol
- Positioned as more cost effective than 3GPP based IoT but with poorer QoS
- Flexible architecture, from on-site coverage, to city to national. Private networks possible



Source: https://www.lora-alliance.org/

- Claimed 32 LoRa operators, e.g.
  - Swisscom – Switzerland (national)
  - Orange France – France (national)
  - SK Telecom – South Korea

LoRa – Technical Summary

Item	Battery powered sensor	Battery powered actuator	Mains powered actuators
UE Category	A	B	C
MCL	157dB @ 250bps 138 dB @ 5470 bps 120 dB @ 50000 bps		
Bandwidth	125KHz/250 KHz		
Peak Data Rate UL&DL	50,000 bps		
Power Class	Max +27 dBm (EU 893.4 - 869.65 MHz)		
Target Battery Life	10 yrs		N/A
Security	128 bit AES		
Latency	UL ALOHA Followed by DL	UL ALOHA periodic DL	UL ALOHA Continuous DL

Sigfox

- Ultra narrow band technology, proprietary 'device to cloud' system operated by Sigfox
- Unlicensed spectrum (e.g. 868 MHz in EU), limited power and duty cycle < 10%
- Very low data rate and positioned as ultra low cost

- Claimed coverage in 32 countries, e.g.
  - Thinxtra - Australia, New Zealand with Hong Kong to launch June 2017
  - Telefonica – Europe and Latin America.
  - Arquiva – now live in eleven major UK cities.

Sigfox – Technical Summary

Item	Battery powered sensor
MCL	≈160dB
Bandwidth	100Hz
Peak Data Rate UL&DL	12 bytes UL, 8 bytes DL
Target Battery Life	10 yrs
Security	Crypto token, no payload encryption (as an option?)
Latency	Max. 140 messages/day UL 4 messages/day DL (triggered by UL)

Mission Critical Network Resilience Aspects

- In very general terms, commercial mobile networks are optimised for serving very large numbers of customers in the most cost effective manner:
  - Core - likely to be resilient with some power backup
  - Transmission network not likely to have extensive power resilience or dual resilient links
  - Base stations unlikely to have power resilience
- Today's mission critical mobile networks (e.g. TETRA, P25) serve a smaller number of customers but are built with a higher level of resilience
- Commercial rollout of IoT LPWA networks geared to very high volume/low performance
- BUT - starting to see commercial LTE networks being used for mission critical using (e.g. United Kingdom)

LWPA/Mission Critical Fit (Commercial Networks)

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

Mission ‘Assistive’ Applications

- I have used the phrase ‘mission assistive’ for applications that could be used by a mission critical service provider to assist their operations. For Example:
  - Ongoing trial in Scotland[1] for electricity pole early warning device which detects excessive bending on the pole in high winds. This includes an IoT sensor, LoRa LWPA and Solar power
  - Australia – LoRa trial with Ergon Energy[2]
- Potential volume of such solutions could be high

[1] https://www.ekkosense.co.uk/ekkoair-iot/internet-of-things/
[2] http://www.zdnet.com/article/nnn-co-succeeds-in-testing-lora-utilities-iot-network-out-to-30km/

Summary

- This presentation has considered a generic mission critical application which is typical of today's TETRA applications
- Looked at three 3GPP based IoT technologies and two proprietary technologies
- For the generic mission critical application considered
  - commercial IoT LWPA networks are not likely be suitable primarily because of the level of resilience
  - Private LPWA could be suitable but is likely to be more expensive
  - New mission critical use of public LTE may open up opportunities for MC SCADA
- Mission 'assistive' applications could be significant users for IoT LPWA

Contact details

Nick Smye

Principal Consultant

nick.smye@masonadvisory.com

Mason Advisory Limited

12th Floor, Blue Tower
MediaCityUK
Salford M50 2ST
Tel: +44 333 301 0093

www.masonadvisory.com
Registered in England No. 8990928