IoT for Public Safety

Authors: Paul Voskar - Huawei, Harold Linke - PSCE

The *Internet of Things (IoT) for Public safety* white paper describes use cases for IoT in Public Safety. The scope of the white paper is to describe a selection of use cases that demonstrate the potential of IoT using different technologies: licenced and non-licensed as well as standardised and proprietary.
The objective of the white paper is to show how IoT can be used to aid the practitioners in public protection and disaster response in saving human life and help local communities tackle emergencies and dangerous situations, by deploying sensors or devices to monitor the environment (e.g. air pollution, river water level detection, fire, gas detection), or in controlling devices such remotely accessing door locks, etc. The use cases are the result of questionnaires and discussions with practitioners in different fora like the PSCE conference or the PSRG workshops.

Target audience: Emergency services, IoT developer Industry, Standardisation bodies, Policy-Makers

Abbreviations

3GPP	3rd generation partnership project
EC-GSM	Extended Coverage GSM
GERAN	GSM/EDGE Radio Access Network
GPS	Global Positioning System
GSM	Global System for Mobile communications
GSMA	GSM association
IoPST	Internet of Public Safety Things
IoT	Internet of Things
NB	Narrow band
NB-IoT	Narrow Band IoT
LIDAR	light detection and ranging
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-M	Long-Term Evolution Machine Type Communications Category M1
MAC-Layer	Medium Access Control
eMTC	Long-Term Evolution Machine Type Communications Category M1
LoRa	Long Range
SIM	subscriber identification module

Introduction

The Internet of Thing (IoT) is changing the world. The network of devices such as vehicles, and home appliances that contain electronics, software, actuators, and connectivity allows these things to connect, interact and exchange data.

IoT is not only for consumers and industry of interest but also for public safety services. These applications are called Internet of Life Saving Things, the Internet of First Responder Things or Internet of Public Safety Things. In this paper we will use the term Internet of Public Safety Things or 'IoPST'.

The Internet of Public Safety Things or 'IoPST' can offer the public safety community new tools to help the emergency services acquire additional information for the emergency services to increase quality of service or help carry out their duties in a more efficient manner.

As an example, IoPST can use sensors in a communications network to provide early warning information on catastrophic events or emergency situations, IoT can offer new capabilities in remotely accessing devices or systems, e.g. cameras, sensors, locks, equipment, etc. When these devices are connected to the internet or via a dedicated radio or cellular network, remote monitoring, diagnostics and control can become a reality. Implementing innovative applications, and making use of dedicated IoPST hardware networks, will give the emergency services potentially lifesaving tools that they can use.

In this white paper we will briefly introduce several communication technologies that may be used for IoPST applications and describe several use cases where IoPST could provide advantages for public safety services.

The objective of the white paper is to show how these IoT technologies can be used to aid the practitioners in public protection and disaster response.

Description of IoT Technologies

NB IoT

Low Power Wide Area Network (LPWAN) is a long-range, low-power, and low-cost wireless technology that has gained interest from both the academia and industry.

NB-IoT is a LPWA licensed spectrum wireless access technology, which offers a wide range of advantages, including a battery life of up to 10 years, a radio link budget gain of 20dB over conventional GSM networks, and support of more than 100,000 connections per cell, at a very low cost ($5 per device).

NB-IoT has been standardized by 3rd generation partnership project (3GPP) in Long Term Evolution (LTE) release 13 [3GPP-NB-IoT], being able to share the high-quality attributes supported by LTE. Moreover, through the use of the LTE security features, enabled by e.g., subscriber identification module (SIM), NB IoT can also offer high reliability and carrier class network security. This means that information can be sent and received reliably, secured and regularly, within a LTE network that has been standardized and deployed globally.

NB-IoT is designed for improved coverage over existing networks, with up to a 20dB gain in link budget. This means that in order to reach locations such as indoors or underground it will be much more likely to connect to the NB-IoT network than with other LPWA networks. Planning for installation is thus

simpler and more straightforward due to the large network coverage, and NB-IoT transceivers can be located in convenient locations, rather than having to compromise on gaining network coverage.
According to **GSMA** NB-IoT deployment map [GSMA-NB-IoT], NB-IoT is being rolled out across the world, with 57 commercial Networks, in 38 countries, as of December 2018. As the LPWA market expands, NB-IoT offer the most accessible technology for IoT connectivity in several Smart Grid/Smart Energy application area so far.

NB IoT supports **three distinct modes of operation**:

A stand-alone mode; this utilises spectrum currently used by GERAN systems as a replacement of one or more GSM carriers.
Guard band mode; this will operate with the unused resource blocks within a LTE carrier's guard-band.
In-band mode; this mode of operation uses resource blocks within a normal LTE carrier.

For NB IOT, stand alone and Guard band deployment options offer the best performance in terms of improved indoor coverage; but FDMA (GSMK) can offer improved power consumption plus savings in terms of lower costs compared to stand alone and guard band modes of operation.
NB IoT can reduce its data rate so as to provide a more robust connection, when coverage is poor, the data will still flow, albeit more slowly. This provides deep coverage, allowing penetration into buildings.

LTE-M

LTE-M (strictly LTE category M1, also referred to as eMTC) is based upon the standard LTE wideband radio interface but includes IoT enhancements for battery life and coverage. It uses a narrower radio frequency bandwidth which allows the chipset to be simplified. Data rates are slower than 'standard' LTE but faster than NB-IoT but the trade-off is that the range (coverage) is slightly worse than for NB-IoT. It is expected that in the LTE-M can be implemented in the radio access network and core network as a software only upgrade.
Similar to NB-IoT it is designed to support a battery life of up to 10 years.
LTE-M has been standardized by the 3rd generation partnership project (3GPP) in Long Term Evolution (LTE) releases 12 and 13. It has similar LTE security features to NB-IoT and uses licensed spectrum.

EC-GSM

EC-GSM brings targeted improvements to lower radio layers of GSM/GPRS/EDGE networks and is intended for those operators that don't have LTE networks. This includes the introduction of a security framework that is comparable with LTE.
Range (coverage) is similar to NB-IoT and EC-GSM is designed to support a battery life of up to 10 years.
EC-GSM has been standardized by the 3rd generation partnership project (3GPP) in Long Term Evolution (LTE) release 13 and uses licensed spectrum.

LoRa

LoRa (short for Long Range) is an open standard LPWA specification intended for battery powered devices. The specification is owned and maintained by an organisation called the LoRa Alliance and its members develop the higher-level protocols which define device interoperability and data transfer between devices and the user host server.

LoRa uses an adaptive rate spread spectrum technique developed by Semtech, which is a French semiconductor company. The range depends upon the data rate used and at the lowest data rate the link budget is estimated to be approximately 7dB worse than NB-IoT.
According to the **LoRa Alliance** (as of March 2018) there are 76 LoRa operators worldwide and LoRa networks in around 100 countries
Three different types of devices are supported depending upon the required downlink latency and battery life:
Class A – intended for battery powered sensors. Each uplink transmission (using random access) is immediately followed by two downlinks receive windows. Downlink transmissions that miss these windows will have to wait until the device is next active. This is the lowest power mode, but it has highest downlink latency.
Class B – intended for battery powered actuators. This has additional downlink windows compared to Class A and so this mode requires more power but has lower latency.
Class C – intended for mains powered actuators. Class C have nearly continuously open receive windows, only closed when transmitting. So, these have the highest power consumption but the lowest latency
It is claimed that Class A and B devices can achieve up to 10 years battery life, but of course (as with other LWPA technologies) this is very much dependent upon the amount and frequency of data.
LoRa has a very 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 and private LoRa networks have also been implemented.
AES 128-bit encryption is used to protect the MAC layer over the air and the payload is end-to-end encrypted.
LoRa positions itself as more cost effective than 3GPP based IoT but with with a poorer quality of service.
LoRa uses unlicensed spectrum (e.g. 868 MHz in EU). Unlicensed spectrum has no statutory protection from interference and, in order to allow multiple users and wireless technologies to co-exist in this shared spectrum, there are limits on the power and duty cycles that can be used. For example, in the European Union the LoRa specification limits the duty cycle to 1%.

Sigfox

Sigfox is a company that offers a proprietary 'device to cloud' wireless network through local operator partners. The core network is cloud based with customer's back end systems connected using HTTPS technology. Sigfox's aim is to offer a global, simple, ultra-low-cost and low-power connectivity solution for large numbers of objects or 'things'. In addition to its core IoT connectivity service, Sigfox offers a range of value-added services to support the deployment and adoption of mass IoT solutions
According to Sigfox (as of February 2019) 60 countries have Sigfox coverage with an area of 3.8 million Km^2.
Sigfox uses an ultra-narrow band (100 Hz) proprietary technology to send very small packets of data (12 bytes on the uplink). Each transmission is repeated three times on different frequencies and can be received by any Sigfox base station within range. Such frequency and spatial diversity can increase the robustness of the transmissions. The Sigfox link budget is estimated to be approximately 4 dB worse than NB-IoT.
Each message to be sent or received by the device contains a cryptographic token that is computed based upon an authentication key that is provisioned during the manufacturing of the device. There is no payload encryption over the air.

The Sigfox network is very much optimized for large numbers of small messages and in order to achieve this it limits the number of uplink messages to 140 messages per day and 4 downlink messages per day per device.

It is claimed that Sigfox devices can achieve more than 10 years battery life, but of course (as with other LWPA technologies) this is very much dependent upon the amount and frequency of data.

Sigfox uses unlicensed spectrum (e.g. 868 MHz in EU). Unlicensed spectrum has no statutory protection from interference and, in order to allow multiple users and wireless technologies to co-exist in this shared spectrum, there are limits on the power and duty cycles that can be used. However, in practice any duty cycle limitations are unlikely to be a problem given the very low volume of messages that can be sent.

IoT Use Cases for Public Safety

The following use cases for IoT in the public safety area have been the results of several workshops with practitioners executed by PSCE and PSRG.

Mountain Rescue (example UK Lake District)

The Lake District in the UK is a mountainous area in the North West of England that covers ca 2,300km^2. It attracts more than 20 million visitors each year. Outdoor sports are a major attraction. The area is prone to changeable weather and heavy rain. In 2011-2015 there were between 425 and 535 incidents annually. The type of incidents varies widely from hikers lost in snow, to fatal falls, suicides, and flood related accidents. There are 12 autonomous mountain rescue teams, mainly relying on volunteers, but collaborating closely with the formal blue-light response services, local authorities and social services, local hospitals.

Key challenges that could potentially be addressed by IoT include equipment management, supporting a new approach to search and rescue and the 'rest of the world' problem, augmenting the environment.

Equipment management: Each team has a large amount of equipment designed for a wide variety of emergencies, some of it like opiate drugs have to be kept locked and each use recorded. The teams often have to carry equipment 'just in case', because when alerted they do not know what kind of incident it is, often into environments with little infrastructure in bad weather, not knowing which type of equipment will be necessary for the kind of emergency they are likely to find (e.g. if victims have suffered broken bones, drugs may be needed, if it's a person who has suffered a heart attack or a person with hypothermia, blankets and a stretcher are needed). Meticulous storekeeping is essential, and difficult because of the amount of equipment. Sometimes multiple incidents in adjoining areas occur. There are inefficiencies in carrying equipment that may not be needed. IoT could support stock-keeping, coordination of transporting equipment, more agile exchange and mutual support between teams and multiple incidents. In addition, some victims carry some equipment themselves (e.g. blankets, tents). It would be helpful to be able to know what they have. There may be potential in rapidly delivering some equipment by drone if a person's location is known.

Rest of the world problem: In the first few hours after a person has been lost, and when their mode of transport is known (e.g. they are on foot from an abandoned car), it makes sense to search an area within a specific radius. As time goes on, and a person (e.g. an elderly resident or visitor with dementia, or a person suspected with intentions of suicide) might have taken public transport, they could be anywhere, and the search within the radius becomes less meaningful. IoT could be used e.g. to activate facial recognition within an area or on public transport, elderly persons or persons with dementia could carry location sensors that could be activated when lost.

Augmenting the environment: There are areas where hikers get lost regularly. For example, as clouds descend and visibility is reduced, hikers on 'Crinkle Crags' are likely to lose their way. Many visitors to the area embark on hiking tours ill equipped and unaware of the dangers. If sensors could be (very subtly!) embedded in the environment so that way markers could be activated when visibility is reduced beyond a threshold, some of the emergencies that result from hikers getting lost could be avoided.

Early fire warning and fire monitoring

Effects of natural and human caused emergencies and disasters are directly manifested in terms of loss of human lives, damages to infrastructure and in long-lasting economic negative impacts. Forest fires can occur due to human factor, but more often are initiated due to high temperatures during summer times. Forest fires can spread very quickly and affect very large areas and cause extensive destruction before fire fighters gain control of the situation/event. It is thus critical to detect and locate fire (source) as early as possible. This can be done by tracking/monitoring and correlating relevant parameters, such as temperature, relative humidity, Carbon monoxide and dioxide with suitable and geo-localized sensors. Moreover, it is also possible to track unusual behaviour (e.g., movement) of wildlife (i.e., animals) by either motion sensors strategically distributed in forest, or using GPS sensors (for location and time) and accelerometers (walking, jogging, running) placed on target animals ([1], [2]). Unusual animal behaviour is expected during fires, and thus the animal location and movement can be correlated with the source of danger (i.e., fire).

For obvious reasons, narrow band IoT devices offer a potential and necessary solution to achieve the above mentioned. Their very-long battery times and low power consumption would require minimal stress to animals and minimal efforts from humans (i.e., only when placing sensors). Moreover, radio transmission capabilities would provide data in real-time, while significant number of connected devices is required due to large forest area coverage. NB IoT device networks could be either used as a stand-alone solution, or applied in combination with other sensing methods and approaches for fire detection (e.g., optical and thermal camera systems, remote sensing techniques) [3].

Extreme environmental events and more extreme weather are expected to increase in frequency in future, and with rising temperatures forest fires will only be more frequent [4]. Sensor networks integrating narrow band IoT devices thus need to be strategically distributed to protect not only the forests, which are crucial parts of our environments harbouring animal and plant life, but also to provide early warnings for human dwellings in vicinity of forests.

Water level metering

Effects of natural and human caused emergencies and disasters are directly manifested in terms of loss of human lives, damages to infrastructure and in long-lasting economic negative impacts. Flooding is one of the costliest disasters, as human dwellings often tend to be either at river coasts or close by, and thus are vulnerable to overflowing of water onto land (i.e., into cities). Moreover, extreme environmental events are expected to increase in frequency in future [5], thus including even more potential flooding of ever spreading cities. These developments require implementing and establishing measures for more resilient cities, including critical activities such as monitoring river flows, integrating early warning systems, as well as response to ongoing emergency flood situations.

For a successful realization of these activities, numerous sensors for delivering real-time data from the field are necessary. Moreover, it is urgent to have sufficient and meaningful/strategic spatial distribution of sensors (e.g., along the river bank) that provide accurate and reliable measurements in relevant time-spans. Different sensor technologies are available to measure flood-relevant parameters, e.g., water level, water speed/flux, rain amount (water level sensors, pluviometers). Further, due to the nature of flooding and river banks topographies/accessibility, it can often be hard to reach spots for proper sensor placement, thus requiring long sensor life-times (and minimal replacement efforts after the initial placement).

Narrow band IoT devices are expected to be self-contained monitoring devices capable of having own power source, i.e., very long battery life, radio transmission capability secured from interception and tampering, and which is low cost and sufficiently portable to be moved when required, with minimum or none occurring issues. They thus meet the criteria for a flood monitoring and early-warning networks for flood-related events/disasters, and thus are the perfect candidates.

Flash flooding is an increasingly common occurrence in many areas. For example, cities like Lancaster in the North West of England experience extremely rapid onset of flooding. And because major roads are situated in the valleys, between watersheds, whole areas can get cut off. Sensors positioned high up in the feeding areas of water courses could provide very early warnings of flooding risk. Also, after the flooding, the emergency staff have to check all properties whether they are safe to move back into. This is a time consuming and labour-some process, as residents must be contacted, transported to the property if they have been evacuated, and properties need to be inspected internally. Sensors embedded in people's buildings would help post-flood recovery assessment. However, this poses ethical issues, as people would not want flooding sensors in their buildings as that would mark their properties as at risk and make them more difficult to insure or sell. Mobile sensors could alleviate some of those issues.

Sensors for Landslide Monitoring and Alarming

Landslide is a type of a disaster in which a part of a ground surface experiences "unintended" downslope movement due to build-up of specific conditions including type of soil, unusual increase of water content in soil due to heavy and extensive rain, and deforestation that eliminates natural defence against such events. Landslides occur around the globe, and since the climate change causes more extreme weather, the conditions for landslide events are getting even more frequent. For example, deforestation occurs due to human factor, as well as due to other disaster types, e.g., wild fires that eliminate vegetation, expose large spatial areas and thus make them very vulnerable when heavy rain is expected. Finally, landslides cause extensive damage to infrastructure and traffic networks (i.e., roads, rails) and thus endanger human life and cause heavy economic burden.

Currently reliable techniques for monitoring such events are rather expensive or technologically limited (e.g., geodesic methods, remote sensing using, e.g., LIDAR's). There is naturally a demand for methods for data collection devices that are both low-cost, low-power and reliable. Moreover, there are efforts to establish active wireless sensor networks for monitoring and potentially triggering alarms when land movement is sensed. Narrow band IoT can certainly play this role, as it offers sensor technologies with very-long battery times and low power consumption, as well as radio transmission capabilities for data provision in real-time. Again, NB IoT device networks could be either used as a stand-alone solution or applied in combination with other sensing methods and approaches for landslide monitoring and alarming.

Air pollution detection

Today large cities have increasing large amounts of air born pollution, invisible and damaging to human health. Efforts to reduce pollution levels are an important objective of cities officials and governments. To tackle air born pollution within our cities or in our country side one first needs to understand the levels of pollution and also ideally the distribution of the pollution present in the city, plus the type of pollution present (Co2, NOx, smoke particulates, etc.). This method can also be used and utilised by the emergency services to monitor smoke in a fire situation, and whether this is within a city centre environment or in the county side within a forest.

Sensors that monitor pollution levels linked into a sensor network distribution within, say a city, can be utilised to carry out this task. But there is a need to communicate back this information to a central control centre for analysis on a regular basis with and in a secure way. This information can then be used by local authorities or the emergency services.

A simple way to do this is to have a self-contained monitoring device capable of having its own power source and with radio transmission capability, that is secure from interception and tampering, is low cost and has a very long battery life, and which is portable so as to moved when required, with a minimum problems.

IoT can perform this role; an IoT device connected to pollution measuring sensor or sensors, package into a unit and installed in strategic positions with a city or in a forest, can monitor pollution levels, and feedback this data 24/7 for many years to the authorities helping to build a picture of the pollution levels over time within a city or at other locations and alert the authorises of peak levels of Pollution. This information will be invaluable for city planners and or the emergency services to be able make decisions if there is forest a fire or to make traffic management decisions within a city, etc. to protect the environment and to create a safe environment for the inhabitants.

Using NB IoT fulfils all these requirement, of a low cost, low power unit with very long battery life (10 years) the technology that can be self-contained, portable, with radio capability connected to a dedicated Cellular network offering secure communications, so when coupled to a sensor sensors can be installed at strategic positions with a city and removed and moved to a new location with ease, enabling a more complete picture of pollution information to be gathered.

Creating a NB IoT pollution sensor network that is self-contained and which can be placed at strategic positions within a city or within a forest or at other key locations would allow the authorities (e.g. health services, local authorities for the management of the traffic) or the emergency services to monitor pollution, allow pollution levels and its distribution to be determined to provide a complete picture; this will help the authorities or emergency services make informed decisions and when necessary, make key decisions quickly in terms of e.g. a forest fire or a chemical spill.

Smart Locks

Today when a fire starts and spreads within a large building especially a large residential or commercial tower block, fire/ smoke alarms activate warning of fire/smoke. The fire service will be alerted. The fire service would ideally like to manage events within the building, such as monitor the spread of the fire/smoke and manage the safety of the residence.

IoT can be used to help the fire service, by using Smart Door Locks; this would offer remote access to key door within the building, so that emergency services could either monitor or even control the opening/closing of key doors to try to aid residence escape from fire/smoke.

NB IoT is ideally suited to be used in a Smart Lock application as it offers very low power consumption, is self-contained, offers high security and is very low cost, plus it can be part of a secure Licence radio network.

A NB IoT device can be imbedded into a Smart Lock mechanism inside a door with its own power source (lasting many years, dependent on use), and can provide a way to monitor or even control the door lock activation, remotely.

The *Smart Lock* is a useful aid for public safety. One can use smart locks within buildings, such as office or residential buildings, to give, for example the emergency services the ability to remotely access key locks within that building, to determine whether a door is (open/closed), also it is possible to offer the ability to open or close key (fire) doors remotely, useful for slowing the spread of fire. If a building is equipped with smart locks the emergency service can have a valuable tool to help ensure the safety of residence of large buildings.

Critical infrastructure protection (example Wooden poles used for electricity transmission lines)

Wooden poles used for electricity transmission lines are prone to rot and eventually will suffer catastrophic failure with a consequential power outage to customers. For lines in remote areas, where there can be hundreds of poles, physical inspection of the poles is very labor intensive. The solution is to use a low-cost device with a very sensitive motion detector that can detect abnormal bending of wooden poles when stressed by wind before they fail. A central monitoring application receives the data from the poles and can identify vulnerable poles in time for the utility to replace them before they fail. In order for such an application to be viable the cost of the sensor and communications channel needs to be very low.

Other use cases

In the several discussions with practitioners additional use cases were found that are not described in detail in this white paper.
Please find below a brief list of the use cases proposed.

- Automated external Defibrillators (AED)
  - Management of the defibrillator
    Sensors may provide information if the defibrillator is used and issue an alert
- Alerting
  - Automatically detect critical situations
    e.g. detect shootings using noise detection sensors
  - Tsunami /earthquakes early warning
  - Early warning on forest fires using sensors
- Avalanches
  - Using snow movement sensors to detect avalanches as early as possible
  - Detecting victims in avalanches
- Border
  - Use Movement sensors and intelligent cameras to detect unlawful border passing
- Cameras
  - Body cameras to protect the first responders
  - Public cameras to detect problems
- Crowd
  - Control of crowd using cameras or other sensors
  - Counting number of crowd members
  - Use sensors and behaviour prediction to detect upcoming problems
  - Infrastructure monitoring
  - Access control to restricted areas during demonstrations
- Use of Drones
  - Autonomous drones to carry various sensors
  - Bring AED (Automated external Defibrillator) to a patient
  - Bring special goods to otherwise unreachable places
  - Monitoring of security and safety
- Equipment
  - Management of batteries
  - Management of equipment in police car

- Fire
  - Fire detection
  - Smoke detection
  - Gas detection
  - Forrest fire warning
  - In door localisation for fire fighters
  - Medical sensors for firefighters
  - Temperature sensors on firefighters
  - Early fire warning and fire monitoring by monitoring animal movement
- Floods
  - Automatic Flood alerting
  - Water level metering
- Monitoring
  - Monitoring during a mission
  - tracking of things or people (covert or aware)
  - Electricity power monitoring

Other topics to consider

Ethical, Legal and Social considerations using IoT

The IoT and specifically the Internet of Public Safety Things pose complex ethical, legal, and social challenges and opportunities. This section will discuss aspects of security, privacy, consent, purpose-binding, data-minimization, proportionality, reliability, technology dependence. The aim is to support creative, pro-active, lawful responses that make the most of the potential of IoT in balance with respect for European values and fundamental human rights. A brief review of state-of-the-art technologies that can support high quality innovation in Internet of Public safety Things includes mechanisms such as privacy preserving data processing.

Security

Each component within the system may be vulnerable to attack – there is a threat. These attacks may have consequences. Components therefore have security features that reduce the risk of attack or reduce the consequences of attack – they protect against the threat. Some components are also certified as offering some security, i.e. the component or subsystem will have been tested to show that some attacks are impractical or uneconomical.

The components are integrated form a system. Some aspects of security cross component boundaries, for example, there may be encryption or message validation between some security endpoints, perhaps one endpoint within the sensor and another endpoint within the processing function. These security endpoints themselves may need management, with issues such as key lifetime, certificate refresh, certificate revocation and firmware patching. There are many resources providing further information, checklists of considerations, and details of good practices and processes. One such list of resources from the IoT Security Foundation is here.

Robustness

When considering robustness, it is important to consider both the resilience of the wireless bearer itself as well as the underlying network topology. In terms of the wireless bearer, resistance to interference is important as well as the ability of the remote device to be use multiple base stations in the case that its local/preferred base station is unavailable. The use of licensed spectrum reduces the likelihood of interference compared to using unlicensed/shared spectrum.

There are also likely to be differences between robustness of commercial networks and self-provided networks. The fundamental purpose of a commercial wireless network is to make a profit and so design considerations focus on maximizing revenue rather than necessarily such mission critical aspects as security, resilience and performance. For example an important area is the level of power backup at base stations, backhaul/transmission and core network. Whilst duplicated backhaul links to a base station are common for public safety networks they are move expensive and so unlikely to have been implemented by commercial network operators.

An interesting new development is the use of commercial LTE networks being used for mission critical networks (e.g. United Kingdom). These are likely to require enhanced levels of resilience compared to the normal commercial offering which could also be beneficial for the support of public safety IoT type applications.

Conclusions

Iot in Public Safety is new and has a lot of potential to support public safety operations. The examples described and listed in this White Paper show this potential and are only a starting point. With every discussion about possible usages of IoT new ideas pop up.

From technology point of view the discussions with practitioners show that NBIoT and LTE-M seem to be the most interesting technologies for public safety users even if the use of LORA might be relevant/promising for some cases.

PSCE is also eager to contribute to the political debate on these emerging technologies for Public Safety and to make sure that the requirements of the practitioners are also reflected into the standardization processes.

Therefore, this collection will continue to evolve. PSCE will not only continue to consult practitioners, collect ideas for critical communications IOT applications but will also make them available on its website.

Acknowledgements

The work on this paper was supported by:

- PSCE NB-IoT working group:
  - Ali Helenius, Airbus
  - Andrew Noy, Mason Advisory
  - Ashweeni Beeharee, Catapult
  - Frank Brouwer, Figonet
  - Hans Petter Naper, DSB
  - Harold Linke, PSCE
  - Ivan Gojmerac, AIT
  - Mario Drobics, AIT
  - Jason Johur, Ericsson
  - Jeppe Jepsen, Motorola Solutions
  - Manfred BLAHA, PSCE
  - Massimo Cristaldi, IES
  - Michael Morris, Motorola Solutions
  - Monika Buscher, Uni Lancaster
  - Nick Smye, Mason Advisory
  - Paul Voskar, Huawei
  - Simon Hohberg, MCS Datalabs
  - Razvan Craciunescuo, Teamnet

- Public Safety Communications Europe Forum
- Public Safety Radio Group (PSRG)

Appendixes

Standardisation

Technology	Standardisation status for RAN features	Standardisation status for CORE features	Considerations, Reference to document
Cat-M1	The core part was completed in March 2016 as part of 3GPP Release 13. The performance part is set to be completed in September 2016 and the testing part is set to be completed in December 2016.	The CORE network from 3GPP Release 12 can also be used. However, the further optimisation of the CORE are available in 3GPP Release 13 and they were completed in June 2016.	
EC-GSM-IoT	The core part was completed in June 2016 as part of 3GPP Release 13. Testing and performance parts are progressing, as part of 3GPP Release 13.	Security enhancement and support for non-IP for EC-GSM-IoT are available in 3GPP Release 13.	3GPP GERAN TR 45.820 **Error! Reference source not found.**, section 10. 3GPP TS 43.064 V13.0.0 Overall description of the GPRS radio interface **Error! Reference source not found.**.
NB-IoT	Radio interface progress: The core part was completed in June 2016 as part of 3GPP Release 13 as category NB1. Subsequent releases have seen features including Positioning, Multicast, higher data rates and the new category NB2.	The CORE network is available in 3GPP Release 13, concluded in June 2016	

Spectrum

Technology	Spectrum	Required bandwidth	Considerations
Cat-1, Cat-0 and Cat-M1	Same as legacy LTE Between 450 MHZ and 3.5 GHz	Standalone requires 1.4 MHz bandwidth	Licensed spectrum: already at the disposal of the operators if they support a LTE network. It allows dynamic multiplexing of the resources between LTE MTC and legacy LTE.
EC-GSM-IoT	Same as GSM. 850-900 MHz and 1800-1900 MHz bands	EC-GSM-IoT requires at least 0.6 MHz bandwidth.	Licensed spectrum: already at the disposal of the operators if they support a GSM network. When using 0.6 MHz, packet switched services (GPRS, EGPRS) are supported, since EC-GSM-IoT is intended for M2M/IoT traffic only. When supporting multiplexing with circuit switched voice services, the spectrum requirement is set by the circuit switched operation.
NB-IoT	Can be deployed in existing operators' IMT bands (e.g. 450 MHz to 3.5GHz), Sub-2 GHz bands are preferred for NB-IoT applications requiring good coverage.	180 kHz for in-band and guard-band deployment, 200 kHz for standalone deployment	Licensed spectrum: already at the disposal of the operators if they support a 2G/3G/4G network.

Bibliograpgy

[1] Y. G. Sahin, “Animals as mobile biological sensors for forest fire detection,” *Sensors*, vol. 7, no. 12, pp. 3084–3099, 2007.

[2] J. P. Dominguez-Morales *et al.*, “Wireless Sensor Network for Wildlife Tracking and Behavior Classification of Animals in Do #x00F1;ana,” *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2534–2537, Dec. 2016.

[3] A. A. A. Alkhatib, “A Review on Forest Fire Detection Techniques,” *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 3, p. 597368, Mar. 2014.

[4] E. S. Hope, D. W. McKenney, J. H. Pedlar, B. J. Stocks, and S. Gauthier, “Wildfire Suppression Costs for Canada under a Changing Climate,” *PLOS ONE*, vol. 11, no. 8, p. e0157425, Nov. 2016.

[5] L. Alfieri, P. Burek, L. Feyen, and G. Forzieri, “Global warming increases the frequency of river floods in Europe,” *Hydrol. Earth Syst. Sci.*, vol. 19, no. 5, pp. 2247–2260, May 2015.