WHITEPAPER

ENABLING A MISSION CRITICAL INTERNET OF THINGS

sepura

Going further in critical communications

APPLICATIONS

TERMINALS

SYSTEMS

The Internet of Things (IoT) represents a vision in which interconnectivity is extended from computers to real-life, everyday objects.

The inter-networking of smart devices, vehicles and buildings – embedded with electronics, sensors, actuators and network connectivity to enable the collection and exchange of data – promises to revolutionise the world as we know it, allowing objects to be sensed or controlled remotely, reducing human intervention and improving efficiency and convenience.

While a significant number of applications – such as smart meters, intelligent shopping systems and remote health monitoring – are geared to the consumer, the ability to monitor a network of smart devices and identify issues as they arise is also becoming vital for mission critical users.

But can a ‘mission critical IoT’ become a reality? Can LTE – a commercial cellular standard – really offer the security, reliability and resilience required for critical communications?

PMR AND LTE: THE FUNDAMENTAL DIFFERENCES

Critical communications are typically delivered via professional mobile radio (PMR): specialist networks delivering high reliability and availability, with feature sets that have been built to match the operational practices of mission critical organisations.

The services on a PMR network are designed for command and control operation, focusing on group-oriented services for fast and efficient communications. Designed to provide geographic coverage, rather than capacity, their architecture is equipped to provide a specific grade of service at peak load – queuing, rather than dropping, calls if peak demand is surpassed.

Commercial LTE networks, on the other hand, are designed for capacity, and are typically tailored to population density rather than geographic coverage. LTE standards do not currently support any of the services considered vital for mission critical users, such as group working and direct mode; LTE does not provide enhanced resilience and security.

Work is already in progress to define the next-generation technology for mission critical communications – which, it is widely accepted, will be based upon the LTE standard – but this is due to complete in 2018. It is expected that there will be a significant lag between specifications being finalised and true mission critical products becoming available.

MISSION CRITICAL IoT: A WORK IN PROGRESS

Many mission critical organisations are already benefiting from consumer IoT via networked CCTV, proximity and audio sensors, and building information management data from critical infrastructure and assets, including alarms, door sensors and telemetry systems. Real-time data provided, for example, via social media is also providing increased situational awareness.

From public safety to military, border patrol, surveillance and critical infrastructure monitoring activities, this 'mission critical IoT' has the potential to contribute to the safety and efficiency of front-line users, enabling the assessment of operational efficiency and the detection of changing key performance indicators as well as providing valuable input into business processes.

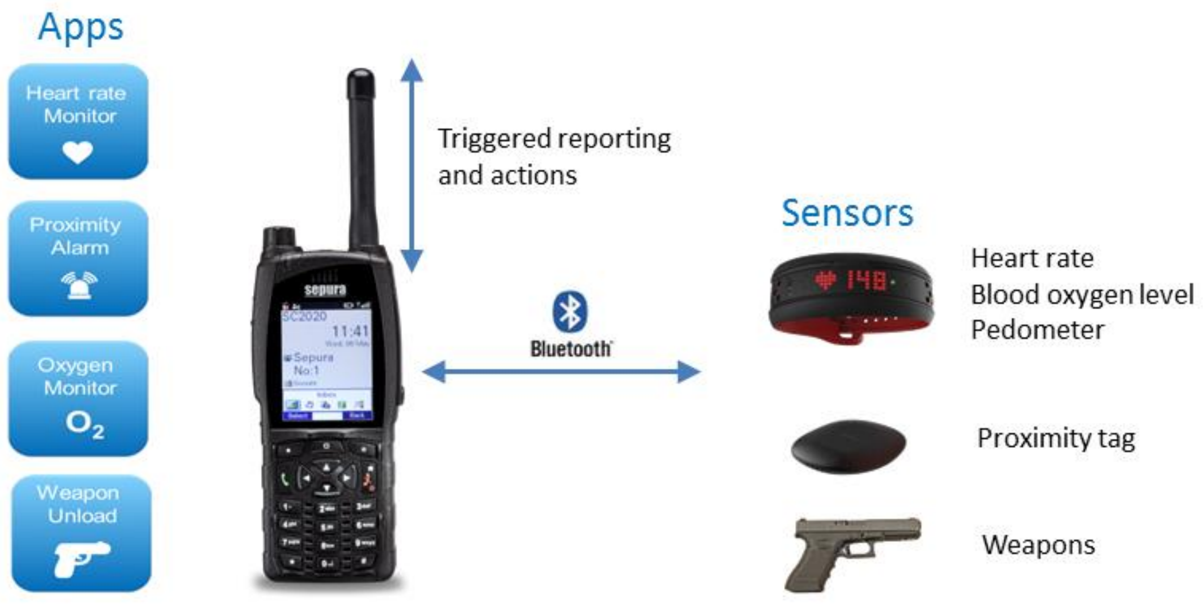
PERSONAL RADIOS AS SMART HUBS

People are one of the most prolific sensors in the mission critical world: they are at the frontline, they relay information to control operators and they rely upon up-to-date situational information to shape their response. Everyday tasks can be simplified – and the risks they are exposed to during those tasks potentially mitigated – via the range of sensors that they carry.

The primary 'sensor' that mission critical users typically *carry* is a private mobile radio, using a technology such as TETRA. Although primarily used for voice communications, these devices provide a good data service that can operate simultaneously with voice services. Importantly, these data services can operate in group mode, which – in command and control environments – is essential for distributing information rapidly and efficiently, particularly during incident response.

TETRA radios have evolved rapidly since their inception and now can be considered smart devices, offering localised connectivity, capabilities including Bluetooth, Wi-Fi and geo-positioning, and sensors such as accelerometers – in addition to wide-area TETRA coverage.

Crucially, these smart radios are also able to run aftermarket applications safely, preserving the mission critical nature of the TETRA services while enabling the creation of a personal IoT platform. A smart TETRA radio can be used as a platform for monitoring sensors and actuators, providing data-based reports to other applications or control room operators, as well as the ability to remotely control the sensors, or even the devices themselves.



TYPICAL USE CASES

Lone worker safety

Every TETRA radio has the facility to check the status of lone workers via simple response requests, but this can be augmented with the use of additional sensors. A heart rate monitor, connected via Bluetooth to an application on the radio, can be programmed to perform a range of actions if the user appears to be stressed, from transmitting a simple data message with an indication of the stress level to the control room or automatically setting up a voice or emergency call to an operator.

A Bluetooth proximity sensor can send a warning signal if the user is separated from the radio, alerting the user – and, if the radio is not subsequently retrieved, the control room. This can prevent the loss of valuable equipment and unauthorised access to secure information, as well as highlighting the potential risk to the user's safety.

Firearm monitoring

Firearms can be linked to the radio via Bluetooth, issuing an alert to the control room if withdrawn from the holster. If the firearm is discharged, an emergency call is automatically initiated – along with location information – ensuring that the incident is recorded and appropriate assistance is dispatched as quickly as possible. Since heart rate typically increases ahead of firearm discharge, monitoring can also be used in conjunction with a heart rate monitor, automatically issuing a warning if pre-defined levels are reached.

Body-worn camera activation

Body-worn cameras can be manually activated whenever there is a need to record an incident or perceived threat. However, linking the camera to a smart TETRA radio – allowing a single press of the emergency button to initiate an emergency call and automatically start recording – not only allows the user to concentrate fully on their surroundings but also ensures an auditable video log for any emergency call. Equally, a linked heart rate monitor evidencing elevated stress levels could cause the radio application to initiate an emergency call and start recording with no user intervention whatsoever.

In scenarios where multiple officers are present, all body-worn cameras in the vicinity can be remotely activated, capturing footage from numerous perspectives and maximising the chance of gathering the required intelligence.

Proximity/location

Whether in urban canyons or industrial locations, the challenges of locating indoor workers can be overcome by pairing a beacon system with an application on a smart TETRA radio. Every time a beacon is reached, the application triggers an alert – using either standard Bluetooth or Wi-Fi technology, or both – via the secure TETRA bearer, reporting the user location.

Some or all of these scenarios could be combined to provide an automated safety service, as well as a comprehensive audit trail.

RELIABLE COMMUNICATIONS AND BANDWIDTH REQUIREMENTS

Like mission critical communications, mission critical applications require reliability, availability and security, which cannot always be provided by commercial network operators. However, where the application is not sensitive or the information from devices is from a public source, it may be possible to combine a secure private networking solution with a commercial service.

LEVERAGING YOUR RADIO NETWORK

Mission critical applications for emergency services rely on real-time data being consistently and accurately transmitted to a server or control room. This is different to the data transfer model utilised by consumer devices, and indicates why a different approach is required.

Normally, mission critical applications may maintain typical levels of traffic throughout the day but, when there is a major incident, sustained peaks can occur.

Consumer networks are designed to cope with occasional data peaks, but these are usually based on 'busy hour' predictions and are able to resort to call blocking if overloaded. They are simply not provisioned to cope with the guaranteed access that is essential for mission critical applications.

Using the data capabilities of a TETRA network for IoT applications would provide guaranteed priority for this traffic, along with an added level of resilience within the network architecture and coverage.

Many IoT devices use wireless spectrum to send and receive data. However, many commercial IoT devices use unlicensed spectrum which cannot be considered to be reliable enough for mission critical IoT as it is susceptible to interference and access cannot always be guaranteed.

This does not mean that Mission Critical IoT should avoid using unlicensed spectrum. Rather, it underscores the need for awareness of its limitations and the capabilities of wireless networks in general. Where availability and security are required, it may be prudent to use a dedicated secure network and, for specific applications that require enhanced security, ensure that device authentication and encryption is applied to protect any information transferred.

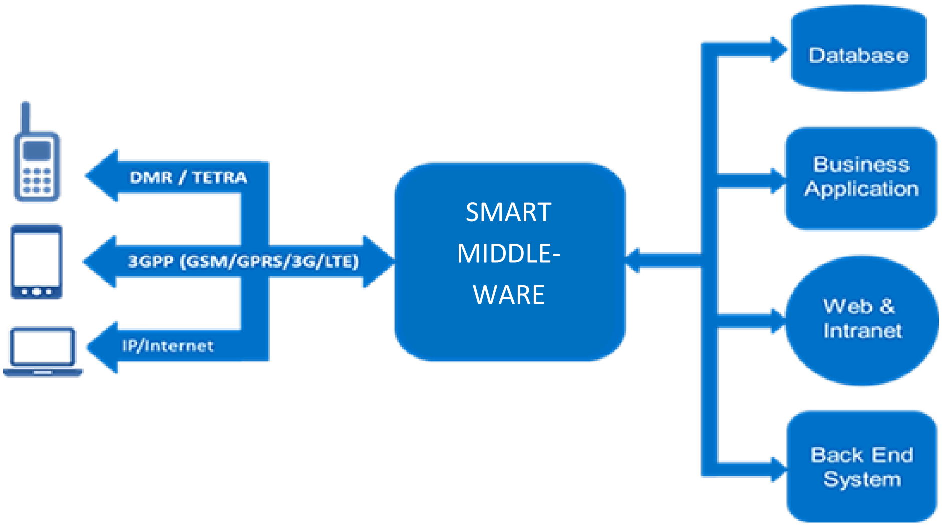
DATA FUSION

For mission critical IoT, it is likely that there will be an unprecedented increase in diverse applications and services with extremely heterogeneous performance requirements. As the general volume of traffic increases, with more connected devices coming online, this will present enormous challenges to fulfil the key performance requirements, in particular for high bandwidth applications.

Many mission critical users have access to commercial broadband services as well as their TETRA service and, over time, may have access to mission critical broadband services. Many IoT devices currently utilise broadband networks either because they need the broadband capability – for video or CCTV transmission, for example – or because the data is not deemed sensitive or its availability requirement is not high.

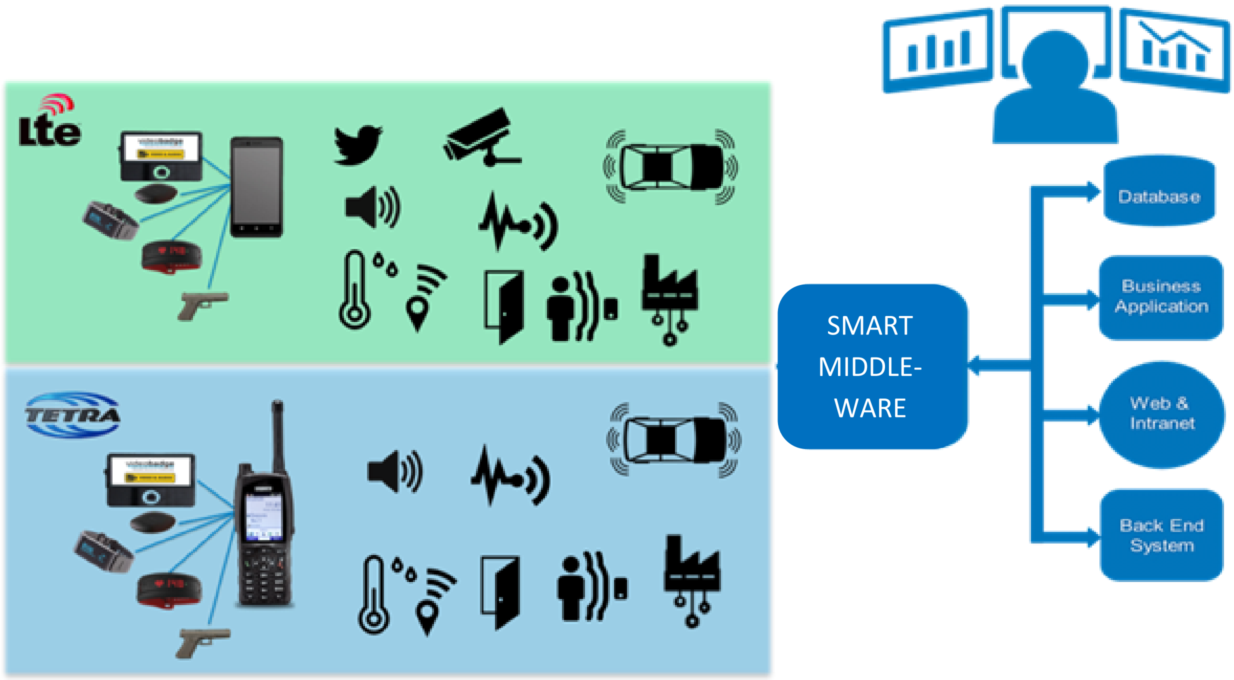
The use of a hybrid solution – consisting of TETRA for high reliability and coverage, broadband for high bandwidth requirements and unlicensed technologies such as LPWAN for commercial IoT devices – is the most flexible approach, allowing organisations to benefit from all of the potential of a mission critical IoT.

The use of hybrid networks requires the ability to decouple the data from the system that generated it, 'freeing it' to be used in a technology-neutral manner. Smart middleware ensures that the applications are not tied to any one technology, allowing the system to send and receive information to any IoT object, regardless of the network.



Smart middleware can also be used to provide business intelligence, correlating data from IoT objects to provide meaningful information for applications and control room users.

As the ecosystem of IoT objects evolves, it is important that this business intelligence evolves in line with user needs, supporting adaptation, management and reorganisation of information sources, devices, and networks autonomously. This will avoid imposing the additional burden of interpretation and analysis of the data on the end users.



CONCLUSION

As demands facing mission critical organisations grow and their operational environment becomes increasingly unpredictable, technologies to monitor critical performance criteria and provide real-time information will become vital to meeting organisational expectations and keeping frontline staff safe.

By exploiting existing voice-centric mission critical comms networks, mission critical IoT solutions will provide the control needed to boost productivity and efficiency whilst provide the necessary awareness to safeguard personnel and critical assets.

To discuss your communications requirements, get in touch with your Sepura contact or visit www.sepura.com

sepura

Going further in critical communications