CRITICAL COMMUNICATIONS TODAY

The global information resource for mission-critical communications

p10

Focus Nordics
The Nordic countries pioneered cross-border TETRA emergency services comms and are now planning transition to LTE

p22

US public safety LTE
The US is building a nationwide broadband network for first responders on AT&T, but other carriers want a slice of the pie

p27

Watching you
Facial recognition technology is improving all the time, but its deployment in public spaces remains controversial

March 2020
www.criticalcomms.com
@CritCommsToday

SUPPORTED BY TCCA 25

PUBLIC SAFETY • TRANSPORT • INDUSTRY

CRITICAL
COMMUNICATIONS TODAY

Editor: James Atkinson
james.atkinson@markallengroup.com

Deputy editor: Charlotte Hathway
charlotte.hathway@markallengroup.com

Sales manager: Andrew Bird
Tel: +44 (0)7967169083
andrew.bird@markallengroup.com

Graphic designer: Jamie Hodgskin
jamie.hodgskin@markallengroup.com

Circulation manager: Paul Creber

Sub-editor: Chris Young

Production director: Richard Hamshere

Managing director: Jon Benson

Chief executive officer: Ben Allen

Reader enquiry and subscription services:
Tel +44 1722 716997
(in the UK, 0800 137201)

Views expressed in this magazine do not necessarily represent those of the editor or publisher. The publisher can accept no liability for any consequential loss or damage, howsoever caused, arising from any information printed.

MA BUSINESS
A MARK ALLEN GROUP COMPANY
www.markallengroup.com

Critical Communications Today
is published by:
MA Business Ltd, Hawley Mill, Hawley
Road, Sutton at Hone, Dartford, DA2 7TJ,
United Kingdom
Tel. +44 1322 221144
Online edition:
www.criticalcomms.com

Twitter: @CritCommsToday

Please read our privacy policy, by visiting http://privacypolicy.markallengroup.com. This will explain how we process, use & safeguard your data

(Print) ISSN 2517-2719
(Online) ISSN 2045-8673

UK Personal subscription rates

Quarterly Direct Debit	£13.50
Annual Direct Debit	£55
Annual Credit Card	£58
2yr Annual Credit Card	£99
3yr Annual Credit Card	£139.50

Subscribe online:
www.magsubscriptions.com
Subscribe by phone: +44 (0) 1722 716997

Printed by: Pensord Press Ltd

recycle
When you have finished with this magazine please recycle it.

The paper used within this publication has been sourced from Chain-of-Custody certified manufacturers, operating within international environmental standards, to ensure sustainable sourcing of the raw materials, sustainable production and to minimise our carbon footprint.

Cover credit: Motorola Solutions

MARCH 2020

6

22

10

27

4 Editor's letter
James Atkinson considers some of the concerns surrounding interoperability in mission-critical LTE networks, products and solutions

6 Who, what, where
The Netherlands transitions to an upgraded TETRA network; Highways England invests in Sepura TETRA radios; Swiss Air-Rescue adopt Hexagon CAD system; Hamburg fire brigades choose Motorola pagers; Nokia SpaceTime analytics trialled on Japanese rail crossings; Klabin implements MOTOTRBO Linked Capacity Plus system in Brazil

8 News
APD awarded control room integration project by the Home Office for ESN; T-Mobile US and Sprint merger brings free 5G first responder offer nearer

9 TCCA news
TCCA has joined a project to create compliance testing for mission-critical implementations

10 Nordics in focus
PMR is widely used across a number of industries in the Nordics and each has a nationwide TETRA emergency services network, but most are looking towards a broadband future

14 Testing MC 4G products
TCCA's Jeppe Jepsen explains why it is so important that an interoperability test and certification process is established for mission-critical LTE products and solutions

16 3GPP SA6 progress
SA6 chairman Suresh Chitturi provides an update on the latest work to develop specifications for mission-critical applications in 4G and 5G

22 MC LTE in the USA
The USA is implementing a nationwide public safety broadband network, but the situation is complicated by other providers offering similar services, leading to concerns over interoperability

27 Facial recognition
Facial recognition technology can help identify suspects and locate missing people, but its use is controversial as it raises privacy concerns

31 Network resilience
PMR networks are hardened to resist environmental damage and deploy redundant switches, links and power, but now commercial 4G broadband networks need to find ways to ensure they also meet mission-critical criteria

Ensuring interoperability

Critical Communications Today editor James Atkinson discusses some of the issues associated with the transition to mission-critical LTE and how to prevent different implementations of MC products and solutions

MISSION STATEMENT

Critical Communications Today provides the global mission-critical community with insight into the latest technology and best practice required to ensure that its members always have access to the instant, one-to-many wireless communications that can make all the difference in moments of crisis.

We are dedicated to providing our readers with the knowledge they need when determining their critical communications strategies and procurements, though delivering up-to-the-minute accurate information on industry trends, developments, and deployments, as well as the latest new products and services. Our journalists are committed to easing out the little details from your peers that will allow you to draw on the industry's collective experience of deploying and implementing new projects and systems.

We work to stimulate and focus debates on the topics that matter most and provide our readers with a means to raise their concerns and speak frankly about their work and the lessons they've learned while delivering the devices and networks that the world's blue light organisations depend on.

Spearheaded by TCCA, the TETRA community put a lot of work into ensuring that TETRA products and solutions could all interoperate with each other. The TETRA Interoperability Certification Process (IOP) provides a series of interoperability tests to ensure end-users can mix and match products from different suppliers and be confident they would all work together.

We are in the early days of transition to mission-critical LTE, but it has been apparent for some time that a similar process is needed for MC LTE. The process will be more complicated, because unlike the integrated approach of TETRA, the hardware and software for 4G are separate. TCCA is leading the way on this, as our interview with Jeppe Jepsen (page 14) reveals.

3GPP provides the specifications for MC LTE standards, so in theory products from different manufacturers should all work together. The problem comes with how the standards are implemented by different vendors and mobile operators. Unless there is a set of standard conformance and interoperability tests that everyone adheres to, there is a real danger that products, solutions and networks will not be able to interoperate.

> “The issue is not a technical one; it is a political and commercial one”

Concerns over interoperability are also considered in our feature on the mission-critical LTE market in the USA. FirstNet is designed to offer US first-responders with a single, nationwide MC broadband network.

However, state and local public safety agencies are not obliged to sign up. Other carriers also offer PTT over LTE services. Not only that, there will be a mix of PTT options: 3GPP-compliant MCPTT, carrier-integrated PTT and over-the-top PTT options. If the goal of full interoperability is to be realised, all these PTT options and the different carriers will also need to interoperate. The issue is not a technical one; it is a political and commercial one.

Elsewhere in the issue we take a look at critical communications in Scandinavia, talk to SA6 chairman Suresh Chitturi about progress in 3GPP on mission-critical specifications, and examine facial-recognition technology and its controversial implementation. Finally, we look at what's required to ensure network resilience in both LMR and MC LTE networks.

James Atkinson

James Atkinson, editor

APD

An NEC Company

INTEGRATED CONTROL ROOM SOLUTIONS THAT HELP YOU PROTECT YOUR COMMUNITY

ENABLING PUBLIC SAFETY IS OUR MISSION.

We want to help you pro-actively support safer communities, and be ready to respond when it matters most. Get to know the public as people, not as incidents. Connect with the community, wherever they are.

CONNECTED TECHNOLOGIES, CONNECTING COMMUNITIES.

- Coordinate people, incidents and resources **from one place**
- Protect the vulnerable with **intelligent contact histories**
- **Track what's important in real-time** with intelligent mapping
- Integrate and **streamline all contact channels**
- Dispatch the right resources, **fast**
- **Link** radio, telephony, CCTV and social media
- Be accessible on **live chat and social media**
- Help manage demand with **AI chatbots**

Visit us at **apdcomms.com**

Who, what, where

EUROPE

The Netherlands switches on new emergency network

The Dutch government has confirmed the successful transition to a new TETRA emergency service communications network.

During the overnight migration, the previous voice network was put on standby while the new C2000 network became operational. The process had been carefully prepared to ensure emergency services provisions continued as normal without any noticeable disruption for residents.

Emergency services carried out their work using alternative procedures and means of communication, including using mobile phones, and the emergency number 112 remained accessible.

Nationwide coverage was restored immediately after the migration was completed.

Highways England invests in Sepura TETRA radios

Highways England has upgraded its critical communications capabilities with the purchase of over 700 Sepura SC20 TETRA radios for its frontline traffic officers.

Highways England manages more than 4,300 miles of road, carrying a third of all traffic by mileage and two-thirds of all heavy-goods traffic. Its traffic officers have a responsibility to help the company keep major roads free-flowing, safe and serviceable. To do that, they need to be able to speak to other patrols and back to one of the seven control rooms, using the UK's nationwide TETRA Airwave network.

Al Edwards, technology operations manager for Highways England, explained: "The SC20 had a number of features that will undoubtedly enhance the safety of our officers when on patrol or attending incidents."

Swiss Air-Rescue service Rega deploys Hexagon CAD

Swiss Air-Rescue service Rega has successfully implemented Hexagon's computer-aided dispatch (CAD) solution.

The highly integrated solution will support the 17,000 missions the agency completes each year, with staff at Rega's command and control centre using Hexagon to support call-taking and incident management.

The new Hexagon solution modernises Rega's emergency call-handling, incident management, alerts, dispatch and post-incident analysis capabilities. It is integrated with Rescuetrack's helicopter tracking software – adding geographic information system (GIS) and geodata management system features. Rega supervisors and officers can now run an integrated system with operational- and information-specific elements.

Hamburg's fire departments choose Motorola pagers

In order to reach their volunteer firefighters in cases of emergency, the fire departments at the German city-state of Hamburg have decided to equip their first-responders with 3,000 reliable and easy-to-use TETRA two-way radio pagers from Motorola Solutions.

The ADVISORTM TPG2200 TETRA two-way radio pager provides the fire departments with optimised availability through the TETRA digital radio network, with high usability, a lightweight but rugged design, IP54 certification, as well as long battery life.

In case of an emergency, volunteer firefighters can quickly read and respond to messages. The pagers provide GPS for location services, allowing the control centre to only send messages to the firefighters that are close to the specific area of the emergency.

ASIA PACIFIC

Odakyu railway trials Nokia's SpaceTime for crossing safety

Odakyu Electric Railway Company in Japan is identifying ways to enhance rail crossing safety using Nokia's SpaceTime scene analytics.

Trials are running from February into March at Tamagawa Gakuenmae No.8 railroad crossing in Machida City, Tokyo.

Nokia's scene analytics will analyse available image feeds, generated by conventional railroad crossing cameras, to detect abnormal events by applying machine-learning-based artificial intelligence. This should identify potential issues in real time.

The Odakyu Electric Railway Company has said it is committed to advancing innovative technology in order to make the Odakyu Line the safest rail company in Japan. It has 229 crossing points across 120.5km of rail track, with 137 radar systems for object detection.

SOUTH AMERICA

Klabin takes connectivity to the forest with Motorola

With 17 plants in Brazil and one in Argentina, packaging paper producer and exporter Klabin owns 239,000 hectares of pine and eucalyptus forests and 216,000 hectares of preserved native forests.

To connect the forested regions with its command centres, Klabin has implemented a MOTOTRBO Linked Capacity Plus system with SLR5100 and DGR6175 repeaters at six signal repeater stations in the company's production plants. Machinery used in the company's forestry operation has been equipped with DGM8000 and DGM8500 MOTOTRBO radios, and staff on the ground now use DGP8550e and DGP5050 handheld radios.

There are more than 700 radios with clear, instant audio and precise GPS positioning.

APD wins UK ESN integration contract

The Home Office has contracted APD Communications to develop critical software to integrate blue light organisations and other public services with the forthcoming Emergency Services Network (ESN).

ESN is intended to replace the UK's existing TETRA-based Airwave network, and the Home Office is leading a cross-government programme to deliver it. It will provide police, fire and rescue and ambulance services, as well as other public safety organisations, with voice and data services.

The contract means APD will create an integration solution to connect emergency services to ESN, with the old and new systems working in tandem. It will pave the way to individual services and agencies undergoing a managed migration to the new advanced communications network. APD is the first supplier to be contracted to deliver ESN integration.

Mike Isherwood, managing director of APD, said: "We are delighted the Home Office has placed this significant contract with us, which reaffirms our position as the control room market leader and as a global control room leader in LTE solutions. It's a significant badge of honour and will allow us to ensure all our customers are at the forefront of technology and operational efficiency, enabling them to employ the most modern methods for interacting with, serving and protecting the public."

The Home Office contract runs to January 2021 and requires APD to produce control room technology, which will be trialled by lead force Thames Valley Police. A subsequent nationwide roll-out is expected to take place in 2021 and 2022.

Isherwood added: "The Home Office has placed its trust in us, on behalf of all the organisations it represents, to produce the control room technology required to connect with ESN. Subsequently it will be down to each individual service to make the transition, supported by our software solution. This is an absolutely critical step towards an exciting future. The primary objective is to continue to protect the public during this migration, ensuring a business-as-usual transition.

"After successful migration, the focus will shift to improving and enhancing services to the public through the use of this next-generation technology to deploy a new wave of applications, such as enhanced location services and live video-streaming, that will help public services to be more efficient, more effective and share information more easily."

APD's mission-critical communications and control solutions are used by more than two-thirds of UK police forces, as well as other emergency services organisations. The company also provides critical software for major transportation hubs, including Gatwick and Dubai international airports and the London Underground.

T-Mobile US's 5G public safety offer a step closer

A US federal court approval in February for the $59bn takeover of US mobile carrier Sprint by rival T-Mobile US has brought the promise of a 5G service for first-responders a step closer.

T-Mobile promised that if its proposed merger with Sprint gained regulatory approval it will offer free 5G access for public safety agencies under its Connecting Heroes Initiative. The carrier previously said that if the merger were approved it "will launch a 10-year commitment – providing unlimited talk, text and smartphone data for state and local public and non-profit law enforcement, fire, and EMS agencies".

However, the carrier has not said whether it will provide the necessary priority and pre-emption services for first responders, or whether it will offer 3GPP-compliant mission-critical PTT services.

On 11 February, a US federal court rejected a lawsuit by 13 state attorneys, including in California and New York, who objected to the deal claiming it would reduce competition and result in higher prices for consumers. The appeal by the states was made despite the fact that the FCC and the US Department of Justice had given conditional approval of the deal.

T-Mobile and Sprint argued that by combining the two companies they will be in a better position to compete with their larger rivals AT&T and Verizon. The judge in the US federal court for the Southern District of New York, who heard the case in December 2019, appears to have agreed and ruled that the merger was not expected to significantly lessen competition and noted that Sprint was in a weak position by itself.

The two companies hope to complete the deal by 1 April, some two years after the merger of the third- and fourth-largest mobile operators was first announced. A number of regulatory formalities still have to be completed before the merger can be finalised. California telecom regulators have still not approved the deal, which may delay finalisation of the merger.

T-Mobile has made commitments that the amalgamated network will extend 5G coverage to 97 per cent of the US population within three years and 99 per cent within six years, as well as making commitments to extend rural coverage to cover 90 per cent of rural Americans.

Madison Square Garden deploys Motorola radios

The Madison Square Garden Company will use MOTOTRBO professional two-way radios at its properties across the country. Beginning this month, a total of 1,100 of the Motorola Solutions radios will be deployed across Madison Square Garden, Radio City Music Hall, Beacon Theatre and Hulu Theater in New York, The Forum in Los Angeles and the Chicago Theatre in Chicago.

At MSG properties, the MOTOTRBO push-to-talk digital radios will be used for discreet and seamless communication between facilities, hospitality and security staff, who work closely in the set-up and production of major events. The delivery and integration of the radios and related equipment will be managed by PMC Wireless.

"Communication and organisation are imperative for putting on successful events at each of our venues," said Ron Skotarczak, executive vice-president, marketing partnerships at The Madison Square Garden Company. "Our partnership with Motorola Solutions will only benefit our operations and improve the guest experience at all our venues."

MOTOTRBO radios are part of Motorola Solutions' end-to-end enterprise communications suite, which helps commercial customers manage disparate technologies and systems. Solutions include two-way radios and broadband devices, robust video security and analytics, dynamic incident management and dispatch software, private LTE (CBRS) and managed and support services.

TCCA joins compliance testing project

TCCA has joined a project to create compliance testing for mission critical implementations.

In recent years, 3GPP has standardised mission-critical features, yet test equipment manufacturers have not implemented mission-critical test cases on their machines. Features that have been standardised include mission-critical push-to-talk (MCPTT), mission-critical data (MCData) and mission-critical video (MCVideo).

3GPP has accepted a change in the approach for mission-critical test cases in response to the gap between standards and testing.

MCS-TaaSting, or mission-critical services testing as a service, aims to fulfil the specific needs of the mission-critical communications community in terms of compliance testing.

An IP-based test simulator will be developed that can be used for the compliance testing of the mission-critical implementations.

The project is being led by Dr Fidel Liberal of the University of the Basque Country, with TCCA, the Public Safety Technology Alliance (PSTA) and Texas A&M University acting as vendor associations and practitioners. The University of the Basque Country will contribute as a mission-critical services expert, alongside Sonim Technologies and Nemergent Solutions. GridGears and TestTree are also participating as testing vendors.

The test set-up will use the TTCN3 code of the 3GPP RAN5 test cases and execute them on an IP-based simulator, which will be made available via a cloud service (the TaaS platform) to any interested testing party.

In addition to the cloud- and IP-based simulator there will also be a possibility to test the mission-critical relevant parts of the LTE radio access. That includes mission-critical QCI bearers, eMBMS and priority and pre-emption.

The requirements of mission-critical users and operators are different from the requirements for consumer device compliance testing, yet some learnings can be taken from those tests. As such, the MCS-TaaSting project will look to build on existing conformance tests from PTCRB and GCF.

The entire set-up will be tested in a test lab environment to check the simulator, the test cases and the processes.

When finalised, the MCS-TaaSting approach should allow cost-efficient regular and frequent testing, re-testing, certification and re-certification of the myriad and increasing combinations of devices, operating systems, middleware and applications.

Photo credit: Johan Eklund

Northern Powerhouse

Recent projects in the Nordic region include the drive for cross-border interoperability with TETRA, ongoing migrations to 4G LTE and more use of hybrid roaming solutions. **Barry Mansfield** takes a look at the progress so far

The Nordic countries have a long-time attachment to Terrestrial Trunked Radio (TETRA), with Finland's plans for its first network dating all the way back to the early 1990s due to the high cost and weak security of its analogue predecessor.

Today the standard is used across the region, not just in public safety but also in mining, oil and gas, utilities and the transport sector. Oslo and Helsinki metros embraced TETRA (in the latter case replacing simple use of mobile phones) to connect control rooms with drivers, rescue and maintenance staff. Then came Helsinki's city tram network.

Several well-known large organisations are happy with TETRA and continue to back it – yet they are still opting to upgrade their existing networks. For example, Danish wind farm operator Ørsted selected Atcom and Celab in August last year to develop an integrated communications system for its HR2 site in the North Sea.

Norway, Sweden, Finland and Denmark all use national TETRA networks for their emergency services communications, but each country is looking at how it can transition to 4G LTE broadband networks

The upgrade will bring improved call quality and data transfer between the site and head office in Esbjerg, while also enabling a better overview of workers' precise location, whether they are active in the port, on board a service vessel or at a wind turbine.

State-owned oil giant Equinor (formerly Statoil) has been using an IP-based TETRA system, including a pager service, on the Johan Sverdrup field. Sogn and Fjordane Energy (SFE) is utilising Norway's Nødnett TETRA network using Sepura TETRA radios supplied by the latter's Norwegian partner Wireless Communications AS.

Elsewhere, Wireless Communications has supplied Sepura STP9000 TETRA terminals to the Norwegian Road Administration (NRA), which also uses Nødnett. This has enabled NRA to extend coverage in mountainous parts of the country, replacing an old analogue system that failed in tunnels and suffered with limited signal range, leaving many

> **Before the adoption of the ISI standard, interactions were more complicated**

of the region's skiing villages without any coverage. The Haukeliester traffic centre now has direct contact with all maintenance staff, since radios are installed in each vehicle.

Cross-border interoperability

The Nordic region is the first in the world where multiple countries have implemented cross-border interoperability, including common talk groups for public safety users. Norway, Sweden and Finland have their own national TETRA networks for public safety communications (known as Nødnett, Rakel and Virve respectively).

A new cross-border system established between all three countries in early February last year is based on the standardised Inter-System Interface (ISI) functionality, enabling police, rescue, customs, defence forces and border guards to communicate effectively.

This co-operation has been particularly useful along the sparsely populated 1,010-mile (1,630km) Norway-Sweden border, where public safety personnel have a tradition of collaborating with peers in the neighbouring jurisdiction.

Before adoption of the ISI standard, interactions were more complicated due to the absence of any common communications system. The Virve network (37,000 users) was first connected to its Norwegian equivalent, Nødnett (55,000 users), in November 2018, while Rakel (80,000 users) and Nødnett had been connected earlier in 2016/2017.

Despite the much-vaunted success of the initiative, a great deal of user preparation and training was involved; users from each country had to agree on common procedures, as well as learning how to use the system.

"We've learned that it's important to facilitate meetings between the users from the different countries, and encourage them to perform exercises," says Nina Myren, deputy head of department at the Department of Emergency Communications in the Norwegian Directorate for Civil Protection (DSB), which oversaw the deployment.

The main users – police, health and fire services – had different ways of going about this, so DSB has offered continued support when needed. "It was a complicated project to establish ISI first time," admits Myren. "It involved two vendors, two operators and user representatives from each country. As with all development projects, there were some issues. But the co-operations went really well between all participants."

Crucially, the users did not have to purchase new terminals – these simply required a software upgrade and to be programmed with the correct talk groups.

Tapio Savunen, Finnish manager for Airbus's Secure Land Communications, has welcomed the shared network model – and co-operation over organisational boundaries – as a good foundation for future development of the sort of mission-critical mobile broadband (MCMB) services that can be delivered by 4G LTE.

Of course, the evolution towards MCMB solutions puts a question-mark over the future of ISI itself. "In the distant future when all countries have been completely migrated to MCMB solutions, the ISI likely will be replaced with a 3GPP-based solution," reckons Savunen.

However, he expects the transition phase to be difficult, since the process can take several years even within a single country. There also remain significant coverage issues in areas with low population density and the mountainous regions of the north, causing governments to search for alternative solutions to build satisfactory radio connectivity.

The possibilities around satellite communications have gained some attention, most notably in a report from October 2019 ordered by Finland's Erillisverkot and written by research organisation VTT.

Satellite future?

The VTT report recognises that the rough baseline for an acceptable service delay is the observer's ability to perceive response time. The response times of human senses are in the order of ~100ms, ~10ms and ~1ms respectively for auditory, visual and tactile information.

For a mission-critical services (MCS) user, it is vital to experience an instantaneous reaction after a service-calling button is pressed in an end-user device to avoid any extra delays while conducting a time-critical mission. In addition, a high service availability close to the 'five nines' is of paramount importance.

VTT surmises that "space communications can become a good candidate for MCS, provided the performance is sufficient and there is an effective integration solution available". In addition to voice services, satcom technologies have been used previously for population early warning systems, of which Cospas-Sarsat is a strong example.

This system was developed for search and rescue operations and locating emergency beacons in maritime scenarios. Many countries have their own emergency population warning systems based on satellites, most famously Japan's J-Alert.

In fact, satellite communications (using Iridium) are already used by several Finnish emergency authorities as a back-up technology and in hard-to-reach locations. However, ▸

The northern regions of Scandinavia are sparsely populated and inhospitable, so implementing comms networks is difficult and costly, but satellites might provide an option in the future

Photo credit: Johan Eklund

IoT prospects

There are possibilities to use the Internet of Things (IoT) in public safety, mainly by equipping first-responders with various sensors and using the information to improve situational awareness without any additional human intervention needed.

Sensors can detect an incident (perhaps a gunshot), track the bodily functions of first-responders or give information about the environment (the chemical composition of smoke, for example). Asset management and asset tracking (inventory management) are other potential applications of IoT and RfID in the public safety domain.

IoT is also the key to realising the vision of Industry 4.0 using 5G and ultra-reliable low-latency communications (URLLC). This is a major subject of discussion at the moment, and Swedish cellular infrastructure vendor Ericsson has implemented early versions of 5G in various facilities (including its own) to boost automation, efficiency and productivity, not to mention helping to cut costs.

the question remains as to whether it is possible to make improvements from a user perspective.

A considerable boost is expected from recent 3GPP/5G non-terrestrial network (NTN) specification activities, which are still at an early stage (as Release 17 efforts begin), to bring the terrestrial and NTN communities closer together. Another milestone will come from low-orbit mega-constellation satellite frameworks.

The road to LTE

In Finland, MCMB project Virve 2.0 is in the procurement phase but should be complete by 2022. Services will be based on the mobile network operators' (MNO) networks. In Finland there is no dedicated spectrum reserved for PPDR, but the spectrum allocated to MNOs will be used.

Finnish legislation obliges MNOs to provide priority and pre-emption services for PPDR users, with a new electronic communications services law coming into force at the beginning of February this year to ensure service availability and quality for users even in times of peak network congestion.

Under the new system there will be one primary MNO, while others will provide national roaming for PPDR users. Suomen Erillisverkot Group, the state-owned operator of the Virve TETRA network, has been appointed operator of Virve 2.0.

Finland is furthest ahead in migrating its emergency services to 4G LTE, but each country is planning to rely on commercial mobile networks for most of the RAN infrastructure

The procurement process is now in the second of two phases – the first covering a dedicated core network for PPDR and MNOs' radio access network services, the second involving mission-critical applications defined by 3GPP standards (MCPTT, MCVideo and MCData).

However, even upon completion it has been accepted that the TETRA-based first generation of Virve will continue to be used by the authorities and security services until at least 2025.

As for Norway, DSB is working on a concept study for long-term replacement of Nødnett (present contracts expire in 2026), provisionally named Next Generation Nødnett (NGN). A dedicated broadband network for mission-critical users is no longer an option since the decision in December 2017 to make Norway's 700MHz band available for commercial operators.

Mobile network operators Ice, Telenor and Telia have proposed a number of solutions, including: a secure MVNO with a state-owned core; a single turnkey provider using its infrastructure and possibly national roaming; and several competing turnkey providers. The most likely option looks like being the 'secure MVNO' model where the state owns the core network.

The Swedish approach to 4G migration differs from the Finnish and Norwegian plans. In Sweden, part of the 700MHz spectrum has been set aside to wait for a final decision on its use. In a report from the Swedish Ministry of Justice, a dedicated LTE network for PPDR use has been proposed.

The spectrum allocation would be 2 x 10MHz with an additional 2 x 5MHz in the longer term – when the current TETRA network, Rakel, is no longer operational. The initial deployment will resemble that of Virve 2.0 in Finland, with the Swedish network starting as an MVNO.

This approach involves a government-owned core network with radio access services provided by MNOs. The introduction of the dedicated radio access network will take place step by step. In Sweden, the final decisions on spectrum usage and the exact operational model of the MCMB network are imminent.

Meanwhile, in Denmark, MCMB procurement is yet to take place. The contract for the Danish TETRA network (known as SINE) is due to expire in 2021 and the

Danish administration is now in the process of tendering communications services for public safety.

The Danish police are already making use of various applications on smartphone devices. These communications (including real-time data, video and images) take place over a mobile operator's LTE network, with a security solution to protect the confidentiality of the data.

Elsewhere, the Finnish police are at the forefront of using drones in everyday operations, with more than 400 trained drone pilots in service and 200 aerial vehicles in official use. Superintendent Sami Hätönen of Finland's Police University College regards their introduction as "the start of a success story".

Meanwhile, some verticals are beginning to make their own moves into 5G independently. For example, Boliden's Kankberg mine in Sweden installed a 5G network underground with the help of Telia in July last year.

Ultra-low latency offers prospects for remote operation of machinery, closer process monitoring, vehicle tracking for safety and higher productivity, local data handling and the introduction of myriad other industrial Internet of Things (IoT)-related applications, such as energy-efficient smart ventilation systems – all on the same voice and data network.

Flight of fancy

Drones are used not only to track fleeing criminals, but also in crime scene investigations, search and rescue operations and crowd surveillance – most famously the Trump-Putin Summit in Helsinki in July 2018, Finland's presidency of the Council of the European Union (between July and December last year) and during Independence Day celebrations.

Drones are equipped with diverse sensors, including video cameras, thermographic cameras, LED lights and more. When Virve 2.0 services are available in Finland, police drones are expected to be used in conjunction with the new network.

The Finnish Border Guard is piloting a more advanced drone solution, following a successful trial period at the close of 2017. While the organisation was known to have around 50 drones in operation at first (utilised in a range of surveillance activities as part of field tests and personnel training), the new system will be activated automatically on receiving an alert from existing border control technology.

This recognition system utilises artificial intelligence (AI) for the interpretation of images in order to ascertain whether a human or animal is moving in the target area.

This device transfers the images over a wireless network to the hub, from where they are transferred to the control room. The Border Guard's Valvonta 2 project last year also explored the possible use of sensor-equipped unmanned vehicles in the northern reaches of the Baltic Sea.

The scenarios covered included surveillance of sea and water areas, waterways and the archipelago, monitoring and checking of containers, oil tanks and other stationary facilities at ports, and environmental accident management. Drones remove the need to dispatch a helicopter or boat.

The other Nordic countries are also quite far along in embracing drones for search and rescue purposes. With the cost of helicopters proving increasingly restrictive, the Norwegian authorities were already exploring UAVs as long ago as 2016.

The first exercise took place in conditions of -15°C in Bykle Setesdal, involving 250 personnel from the police, fire department, International Red Cross, army and air force. The Altura Zenith system gave an aerial overview with optical and thermal cameras – transferring images to base camp and police command using mobile networks.

Drones are being used to patrol long land borders and sea coasts, as well as in cities for major events and drug surveillance

In late 2017, Copenhagen Police deployed a drone as part of its surveillance operations on cannabis buyers in the Christiania area – an effort that resulted in the detention of 60 people on narcotics charges and the seizure of nearly 12 kilograms of the drug.

Since then, UAS Denmark has recognised the appeal of reduced cost (over the use of helicopters) and improved safety offered by drones in road and rail inspections (removing the need for rope inspectors), as well as the capability to monitor longer stretches at lower cost, and for effective image capture even in overcast conditions.

Two-way radio will continue to have a place in public safety and various other verticals for some time yet, but for the emergency services in the Nordics the emphasis over the next few years will be on managing their migration to mission-critical 4G LTE.

Setting off on the right foot

Bringing broadband into critical communications is a complex task. Charlotte Hathway finds out why TCCA is calling for an interoperability certification process

Governments across the world are navigating complex projects to bring 4G/LTE-based services into their critical communications networks. Broadband offers new possibilities for managing and responding to emergency situations but, for the technology to be suitable for mission-critical purposes, more work is needed to ensure services will not be compromised.

Existing narrowband services are underpinned by a TETRA Interoperability Test and Certification (IOP) process developed by TCCA. That process ensures users benefit from the best possible quality and economies of scale. In practice that means devices from various manufacturers can operate securely and safely on infrastructure from numerous vendors. That balance is vital in ensuring emergency services and public safety agencies can choose the right solution for their needs while having confidence they are making secure investments.

Broadband is standardised into 3GPP releases, but mobile network operators (MNOs) implement those standards in different ways when building their own networks. As MNOs are set to play an increasingly vital role in the delivery of critical communications networks, there is a need to open a dialogue to ensure future critical services build on learnings from the roll-out of standards such as TETRA, instead of reinventing the wheel.

TCCA has published a whitepaper to do exactly this. It outlines the requirements, current status and steps needed to be taken within the sector to create a process to certify mission-critical broadband solutions. The paper, titled 'Introduction to Mission Critical Service Interoperability', was driven by Jeppe Jepsen, the organisation's board co-vice chair and director of broadband spectrum.

Critical Communications Today caught up with Jepsen, who explains that understanding what is at stake rests on an awareness of the different environments in which narrowband and broadband systems developed. Jepsen says: "In the past, governments had dedicated spectrum and could build dedicated emergency services networks. They were totally in control of their situation."

When the TETRA narrowband standard was established in Europe, the European community realised its adoption outside of Europe would create a healthy ecosystem that fostered innovation and development. The "real benefit", Jepsen says, of open standards and common spectrum is that companies "competed and worked together to enlarge the market opportunity". All parties – government, the buying community, the supply sector – supported each other and took the time to understand each other's needs. An interoperability programme was then developed to ensure a mix of manufacturers could provide devices and infrastructure that was interoperable.

TETRA has now been implemented in numerous countries around the world, including most countries in Europe, and that commitment to interoperability has given governments and agencies certain assurances.

Jepsen explains: "We are moving into a new world over the next five to 10 years. The majority of governments will not have their own spectrum and cannot build their own networks, so they have to buy service from those who have it – the mobile network operators."

Radically different needs

MNO customers are predominantly consumers and non-critical businesses, and their needs are radically different from those of public safety organisations. Consumer needs often centre on cost, whereas the needs of a frontline police officer or a firefighter going into a burning building, Jepsen explains, are about being "absolutely sure it always works everywhere and without question".

We are now "entering a period where these two sectors have to get to know each other" because governments are procuring services from MNOs that must now "sign up to some conditions" that they were either not aware of, or could have been considered as low priority in the past. One vital area that must be examined is interoperability. The new whitepaper from TCCA lays the foundations for that.

Jepsen says: "About a year ago, we [TCCA] set out to analyse and find out whether we could copy the TETRA IOP process directly, or if we needed to find a different way. This whitepaper summarises the status of that. What we realised was that, with TETRA, the hardware and the software were completely interlinked. If you bought a device from one company, you would have the associated software pre-installed, and the same thing happened on the infrastructure side. With LTE – and later 5G – that is very different.

> “Companies are developing in different directions, which prohibits interoperability. That’s why the paper recommends procurers should make sure they have clear agreements with vendors of what level of interoperability they have to deliver”

“The hardware and the software are separated, which means there are more touchpoints than we had in TETRA. We have pointed out in the white paper that governments and government-assigned operators for mission-critical services need to make sure that all touchpoints are under control. What TCCA can assist with is to make sure that there’s a certification process between the software and the hardware – such as MCPTT [mission-critical push-to-talk] software and the associated server.”

Jepsen cautions an IOP process will not eradicate issues that might arise during implementation. “There are still a number of things that individual service providers in each country will have to manage directly. Each MNO has different business objectives and strategies in specific regions so, even if you take the same system from the same vendor in two different countries, some fine-tuning will be needed. You might think all the networks are the same but, when you dig into it, they are not. It is not enough for a government procurement service to say ‘we want X according to 3GPP release Y’, because that says nothing about how it has been implemented.”

In the context of Mission Critical Services (MCX), this means that LTE or 5G networks could be 3GPP standard compliant, but the different implementations and optimisations mean there could be significant differences in the performance of the network. The TCCA whitepaper points to some 2016 drive testing carried out by Nokia Research Laboratories. The study was not independently verified, but three LTE networks are shown to have latencies ranging from 40 to 100ms. This is just one example of how a network can conform to a standard yet be implemented differently.

Developing a certification process

This complex landscape means that developing an interoperability certification process will be a bigger task than it was for TETRA. The whitepaper explains that interoperability has different meanings to different people; protocol interoperability and product interoperability are not one and the same. TCCA’s definition of interoperability is a combination of protocol and product interoperability that has been certified by a third party.

The whitepaper also lays out where we are with possible interoperability between vendors. ETSI MCX Plugtests are the first verification of implementations of new standards and protocols. They serve as a validation of the standard as well as early practical tests.

Significantly, Jepsen explains: “The plugtests have shown that companies are developing in different directions, which prohibits interoperability. That’s why the paper recommends to procurers that they should make sure, in the contracting phase, that they have clear agreements with vendors of what level of interoperability they have to deliver.”

This adds complexity that could be managed by an agreed interoperability testing and certification system. Without such a system, each service provider will need to test all relevant elements (devices, computers, servers) and their interactions thoroughly. Those tests would then be repeated at multiple locations. This will incur additional costs for suppliers and users, and vendors will likely implement variants of the same products that then need to be maintained separately. An IOP process, TCCA says, will minimise this.

Interoperability can also facilitate cross-border collaboration. Jepsen says: “Cross-border interoperability is clearly a need and a wish. We had that need in TETRA as well. Norway has Motorola Solutions as its supplier, while Sweden and Finland use Airbus radios. Those three countries are interconnected so people can travel across the border if they are allowed to do so. Last summer, for example, Sweden had a lot of wildfires in its forests and Norwegian firefighters used their TETRA radios to come across and assist.”

Interoperability certification is still in its early stages, and TCCA has said in this whitepaper that “TCCA certification over mobile networks is still some time away”. Now is the time to collaborate to ensure broadband is brought into the mission-critical mix in a sustainable, safe and secure way. All stakeholders need to be given confidence in these networks performing as they should – whether that is first-responders needing to relay information instantly, control rooms having visibility over their network, or government agencies knowing their investments are secure.

Broadband offers so much promise for the public safety community. Putting interoperability at the heart of the development of mission-critical services will ensure vendors can deliver on those expectations. We shall certainly be keeping an eye on how TCCA’s certification process develops.

Work begins on Release 17

Suresh Chitturi, chairman of 3GPP's Service and System Aspect 6 (SA6) Working Group, updates James Atkinson on progress to standardise mission-critical services in 4G and 5G

What new features and enhancements were completed in Release 16?

Mission Critical (MC) standards continue to evolve with further enhancements to Mission Critical Push-to-Talk (MCPTT 4.0), MCData (3.0), LMR/LTE Interworking (2.0), Migration (2.0), Railways (2.0) and the MC MBMS (Multimedia Broadcast Multicast Services) API.

Two study items – MC Isolated E-UTRAN Operation for Public Safety (MCIOPS); and the Study into Discreet Listening and Logging for MC Services (MCLOG) – were completed. Two further studies – Study on MC Services support over 5G System (MCOver5GS); and the Study on location enhancements for mission-critical services (enhMCLoc) – are still ongoing and are expected to complete in Release 17.

What are the most important new mission-critical features or capabilities to be added since Release 15 and what do you think are likely to be the most useful to public safety?

Since Release 15, a significant effort was invested in enhancing MCX (Mission Critical Services) capabilities to support railways. There are several unique features, such as functional addressing of users across all call types, and advanced features including call forwarding and IP connectivity. While these are specifically developed for railways, it is expected that they will benefit all verticals of critical communications.

For public safety, one crucial addition is the support for pre-configured groups. This feature enables group re-group operations in a highly efficient manner, which was not possible in the previous releases. Media server has been introduced to support recording of MCData service-related transaction history (such as short data service and file distribution).

With the completion of Rel-16, interworking with LMR can now be considered as fully supported, which has been a strong requirement for public safety agencies.

What is the significance for public safety of the various study items and what follow-on is planned?

During Release 16, several new studies were initiated – MCIOPS, MCLOG, enhMCLoc and MCOver5GS. Taking these in turn:

The MCIOPS study enables the support of MC services in the case of a backhaul failure or a nomadic EPS deployment based on the availability of Isolated E-UTRAN Operation for Public Safety (IOPS). The normative work is in progress and expected to be ready in Release 17.

The MCLOG study enables the support of discreet listening and logging/replay of MC communications. The study considers several scenarios including private and group communications across multiple MC services including voice, video and data. This study is complete in Release 16 and normative work is expected to begin in Release 17.

The enhMCLoc study identifies new use-cases, key issues and solutions for improvements in the handling of the location information (reporting and sharing), and gaps in the existing MC architecture. The study is expected to be completed in Q1/2020 and normative work is expected during Release 17.

The MCOver5GS study aims to identify the impacts and necessary changes in the existing specifications to ensure MCX services can be supported over 5G. A reasonable progress has been made during Release 16, but due to the lack of essential public safety features such as broadcast and D2D support in 5G, the study has extended its timeline into Release 17. The MCOver5GS study is expected to complete in Release 17, followed by normative work in Release 18.

Is work finished as far as 3GPP is concerned on the LMR-LTE interworking function (IWF)? If not, what still needs to be done?

Yes, we can conclude that 3GPP has a fairly complete set of specifications for interworking with LMR with the completion of Release 16. Certain enhancements are possible in the future – typically when new enhancements are made on the 3GPP side, we want to make sure those are also reflected on the interface towards the IWF.

Work still needs to be done to specify the interfaces between 3GPP IWF and the backend of P25/TETRA systems, doesn't it?

This activity is generally considered out of the scope of 3GPP, but I understand there is concerted effort in both ATIS and ETSI to solve the other piece of the puzzle, ie, the interface between IWF and LMR systems.

Suresh Chitturi CV

Suresh Chitturi, director for standards at the Samsung Research Institute in Bangalore, was elected as chairman of the 3rd Generation Partnership Project (3GPP) Service and System Aspect 6 (SA6) Working Group in March 2018. He previously served as vice-chairman of SA6 Working Group, providing a key contribution to the timely completion of mission-critical standards to meet the needs of the critical communications industry. He also represents Samsung on the governing council of TSDSI – the Indian telecom standards development organisation (SDO) – and has previously held leadership positions at several other SDOs, such as World Wide Web Consortium (W3C), Open Mobile Alliance (OMA), Java Community Process (JCP) and the GSM Association (GSMA).

There seems to be some confusion in the public safety community as to exactly where the IWF sits – can you clarify this?

Generally speaking, interworking functions or gateways are seen as an implementation matter. However, strictly speaking from 3GPP's perspective, our responsibility lies in the messages supported on the IWF interface, and this has been fully specified. The IWF implementation must ensure it conforms to the IWF interface as per 3GPP specifications. The implementation of IWF is typically a decision of the MC service provider, who needs to make sure that IWF function is integrated to both the 3GPP system and the LMR system on the other side.

Can you comment on the widening of SA6's brief to include other mission-critical verticals besides public safety?

The Terms of Reference (ToR) for SA6 were modified during Release 15. Mission Critical Applications continue to be a top priority for SA6. However, the charter now includes extending the application-layer standards to other activities such as northbound APIs and other vertical applications and frameworks. For instance, railways is a good example of a mission-critical vertical beyond public safety, and the V2X (Vehicle to Everything) APP is an example of a vertical we have been working on recently to enable integration of V2X applications to 3GPP systems by creating a V2X application support layer.

How does SA6's work fit into the development of the Common API Framework (CAPIF); Service Enabler Architecture Layer (SEAL); and Application Architecture of Edge Apps (EDGEAPP)? What is the significance of these developments?

These initiatives are led by SA6 within 3GPP, and can be categorised into "enabling technologies" for new vertical applications. These activities are particularly important given the strong interest in the industry in deploying new verticals with 5G.

CAPIF provides a unified API framework for third-party applications to discover and invoke 3GPP network functionality, and similarly provides a way for underlying 3GPP functions to register and publish their APIs such that they are discoverable by the third-party APIs. Having a unified framework will enable operators to expose network functionality to developers in a consistent manner.

SEAL provides a common application support layer for verticals. More specifically, it focuses on defining certain essential capabilities such as management of groups, location, configuration, key/ID management and resource management, which can be leveraged by new verticals. Having such a common layer will significantly reduce the time to market for new vertical applications, and we have already experienced this with V2XAPP, and are seeing interest in reusing SEAL for other verticals such as Factories of the Future (FFAPP), Unmanned Aerial System (UASAPP), and 5GMARCH (5GMSG – Message Service for Massive IoT over 5G System), which are being studied in SA6.

EDGEAPP provides an application layer framework or enabling layer for hosting of Edge applications both at the device and the network edge, and interactions between them. The activity focuses on aspects such as service provisioning, discovery, registration, and service continuity across multiple edge networks.

What will be the main areas of focus for SA6 in the next few meetings?

With Release 16 behind us, our top focus will be to progress the Release 17 stage-2 work towards completion in Q3/2020. From mission-critical applications, emphasis will be on the completion of normative work on Railways 3.0, MCIOPS, and MCData 4.0, as well as the recently agreed MCPTT 5.0 work item, which will also address the conclusions from the enhMCLoc study.

We can expect to conclude on the MCOver5GS study as well. Outside MC, we are actively engaged and on track to complete EDGEAPP 1.0, which is a top priority for 3GPP in Release 17 and has been receiving significant interest from the industry. We will also be making progress on other studies such as FFAPP, UASAPP, 5GMARCH and V2XAPP 2.0.

In a nutshell, there is a lot of work riding on Release 17, and we can expect another solid outcome from SA6! Finally, I would like to thank all the delegates and their companies for their commitment and high-quality contributions.

Tait and telent redefine Fireground Communications

The fire rescue experts at Tait Communications have developed a holistic communications solution specifically for the fireground, providing greater protection of firefighters, increased operational efficiency, and ease of use.

Already selected by East Sussex Fire and Rescue Service (ESFRS) to improve the safety of its firefighters on the ground, Tait fire expert and Business Development Manager Richard Russell, and Barry Zielinski, Operations & Services Director at telent Technology Services, explain how fire and rescue services will benefit from this approach.

Can you tell us about the typical challenges of Fireground Communications?

The digitalization of incident ground communications can provide key operational benefits. However, in most cases intelligibility is poor due to limitations of analog radios and the limited transmit power they provide. Careful consideration needs to be taken with regards to the proximity of Breathing Apparatus (BA) wearers, who often have zero visibility, the busy and often noisy environment experienced by Entry Control, discreet communications requirements of officers, and the unique needs of Incident Command Units. Self-Contained Breathing Apparatus (SCBA) masks can create communication challenges as they cover the mouth, which affects the clarity and volume of the voice.

For services such as ESFRS, the key issues that often cause poor communications are acoustic feedback caused by two radios operating in close proximity, difficult to use audio accessories (due to compact size) and battery performance. The culmination of these factors compromises the ability to communicate, the communications flow and, ultimately, the safety of firefighters.

What do you mean by holistic fire ground solution?

At Tait, we've taken a holistic view regarding different users, such as BA wearers, Entry Control Officers, Incident Command Units, and their respective requirements when designing the solution. We have therefore concentrated on accessories like the breathing apparatus, remote speaker microphones, earpieces and batteries. In addition, we've focused on providing a high-performing, stable and reliable connection between the entire fireground and the command control centre.

We also incorporated the ATEX Directive 2014/34/EU for intrinsic safety of the whole SCBA radio and accessory communication solution.

What elements does it consist of?

Tait has taken every step to ensure an optimized solution combining radios, accessories and configurable radio features to complement and enhance operational safety and ease of use for every firefighter.

The radios are available in two variants: ATEX radios for the firefighters, and non-ATEX radios for Incident Command Officers and Entry Control Officers (ECOs). At its core, the solution consists of two key elements, the Radios and Remote Speaker Microphone (RSM), although there are a number of other peripheral aspects too.

No firefighter wants to be caught inside a burning building without communications. As mission critical operations depend on reliable and effective coverage, in addition to ensuring greater transmit power, Tait has developed an optimal receiver design. It's able to outperform analog radios by receiving usable signals as low as -122 dBm, which is typically 4 dB better.

To further enhance the ECO and Incident Command Officers' communication experience, a range of secondary headsets and earpieces have been selected after careful user trials. They provide hands free operation and exceptional voice communication quality to increase speech intelligibility and discreet communications.

The Tait Unified Vehicle solution will enhance incident ground communications by converting the firefighter vehicle into a network of networks. Tait Unified Vehicle combines multiple radio frequency (RF) bearers and integrates these into a compact vehicle mounted mobile radio. Tait Unified Vehicle is capable of Digital Mobile Radio (DMR) and analog radio communications, whilst integrating Wi-Fi, 3G/4G/LTE and Bluetooth.

What accessories do you use for the fire solution and why do they make the solution safer?

Specialized audio enhancements, such as the Tait C-C550 Remote Speaker Microphone (RSM), for both ATEX and non-ATEX radios, ensures that voice is captured loudly and clearly for transmission, as it can be positioned at an optimal operational position for the user and easily connected to a radio with a lead routed through the BA harness.

Dual PTT Buttons have been included with the RSM for enhanced safety, as they make it easier to operate the radio in zero visibility. The two buttons are large, providing excellent tactile feedback, and can be operated with either the palm of the hand or fingertips, providing a significant advantage over the existing RSM. There's also a second PTT button located at the top of the RSM for added safety.

The Tait TP9300 portable radio solution offers a number of enhanced operational features, such as Voice Announcements, which loudly and clearly identify the radio type when first switched on, the selected channel when it's changed, and the battery status, mitigating the risk of user error and enhancing firefighter safety.

Audible battery status announcements indicate current capacity at four stages, indicating how long any radio may stay in use before recharge. As battery performance is a crucial safety component, the solution improves upon ESFRS' batteries and delivers 500mAh (27%) more capacity at 2300mAh. The batteries can also last several hours longer per shift, and the efficient design reduces self-discharge when stowed in vehicles for weeks at a time, which is another key benefit independently verified during early engagement tests by ESFRS project management.

Further safety enhancements of the TP9300 radios include a programmable minimum volume level to ensure received calls will always be heard, preventing users from reducing volume to zero and missing vital calls.

telent recently won the tender to migrate East Sussex FRS from analog to digital DMR Tier II. How will you ensure that the migration goes smoothly and why did telent and ESFRS select the Tait solution for this project?

The solution delivered to ESFRS has been designed in consultation with the service to ensure it can be incorporated seamlessly to meet the specific requirements and challenges it was facing.

Throughout the past 12 months, we have supplied a high degree of consultative support and knowledge transfer. This is based on years of manufacturing and user engagement knowledge, combined with solution design experience, specifically around Fireground Communications, which helped develop proven working solutions for ESFRS.

Following successful simulated incident trials, telent will supply 350 Tait handheld digital radios to ESFRS and provide ongoing support and maintenance of the radios. ESFRS highly appreciated our engagement and I think that this was decisive for them.

telent has already provided successful communications projects to ESFRS, as part of an ICT managed service, so ESFRS was familiar with telent's reliable and trusted solutions for the emergency services sector. The sector is a key focus for telent and we're proud to be able to deliver communication services to support fire and rescue services across the country as they carry out their crucial work.

We are also very pleased to be partnering with Tait for Fireground Communications, as they have vast experience in digital migration projects and have proven that they go the extra mile to ensure optimized solutions for their customers.

Tait and telent will be exhibiting at BAPCO. What can visitors expect to see?

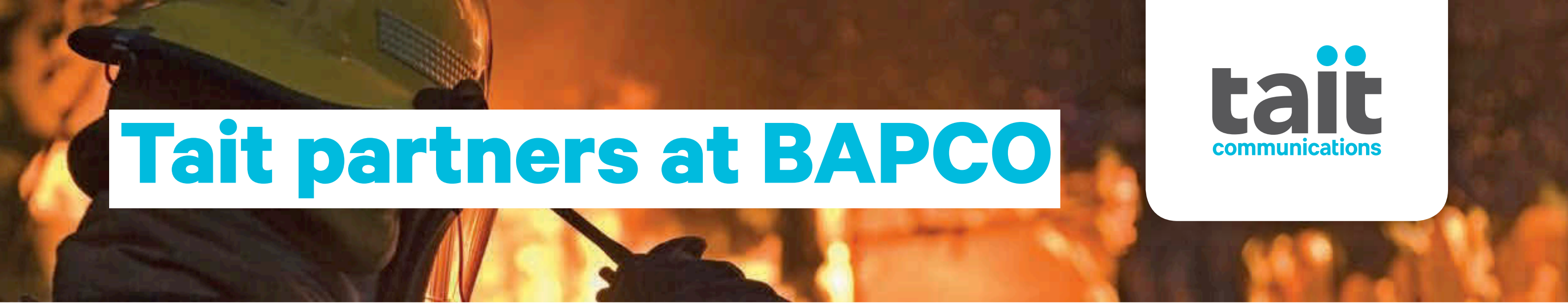
Visitors can book a stand tour and meetings at **www.taitradio.com/bapco** Tait experts will of course demonstrate the equipment used for the fire solution. In addition, Tait and telent are giving a presentation together with Mike Wattam from ESFRS on Wednesday, 11th of March, at 2.30 – 3.00 pm.

Visit us at BAPCO 2020

Tait and telent will be exibiting at BAPCO 10-11 March at Ricoh Area, Coventry.

Tait stand: D40/D50
Tait contact: richard.russel@taitradio.com
telent stand: F2
telent contact: Stephen.Moore@telent.com

BAPCO
The Annual Event 2020



Tait partners at BAPCO

tait communications

omnitronics

Omnitronics is a world leader in the design, manufacture and supply of mission-critical and enterprise communication systems.

Specializing in Digital Radio Management, Dispatch, Interoperability and Radio over IP, Omnitronics products and solutions operate 24/7 in the control centres and radio infrastructures of some of the world's most vital organizations.

Headquartered in Perth, Western Australia, Omnitronics has an international network of offices, distributors and resellers spanning the USA, UK, Europe, Australia and Asia.

The suite of Omnitronics mission-critical Dispatch Systems and RoIP Gateways have formed an integral part of Tait Public Safety solutions globally. Their latest dispatch management system omnicore features public safety specific functionalities as standard inclusions at no extra cost.

Clients including Marine Rescue NSW, Country Fire Authority Victoria, New South Wales Ambulance, and many more appreciate robust and reliable Dispatch, Interoperability, Location Services and RoIP technology that seamlessly integrates with Tait radios and solutions across a plethora of industries.

sonim®

Sonim Technologies. Ultra-rugged mobile solutions built to serve. Built to last.

For over a decade, Sonim has pledged to serve the people who serve us. We proudly invent first-of-its kind technology for extreme conditions, developed with the expertise of people who work in them.

Our determination to be a different type of tech company is something you can count on, just like our mobile devices.

Sonim Technologies is a leading U.S. provider of ultra-rugged mobility solutions designed specifically for task workers physically engaged in their work environments, often in mission-critical roles.

We specialize in workforce-critical communication and connectivity tools for industrial enterprises and public sector agencies including end customers in construction, energy and utility, hospitality, logistics, manufacturing, public safety and transportation.

Our solutions fall into three main categories: ultra-rugged mobile devices, industrial-grade accessories and cloud-based software and application services.

The company is headquartered in San Mateo, California and offers its solutions through the world's leading mobile carriers.

logicwireless™

Logic Wireless was founded in 2004 and is a recognized specialist distributor of business-critical communications solutions, focused on servicing the United Kingdom, Australia, New Zealand and the Pacific Islands region.

With more than 15 years of experience in providing communication solutions for government, construction, event and enterprise clients, we have gained unique insight into the requirements for resilient communications and built a wealth of expertise in our core areas of business.

We distribute and support a range of communication products from major global manufacturers and are the distributor of Tait Communications in the UK and Ireland. This is complemented by our own, Logic Wireless hardware and software solutions.

More details are to be found at **www.logicwireless.co.uk**

Omnitronics, Sonim and Logic Wireless will accompany Tait at BAPCO 2020

BAPCO The Annual Event 2020

tait
communications

THE TAIT TOUGH RANGE HAS GROWN!

INSTANT, RELIABLE COMMUNICATIONS IS JUST THE BEGINNING.

First responders around the world trust Tait for multi-agency coordination in the most challenging environments.

Introducing the new TP9500 and TP9600 mission critical portable radios, featuring:

- Exceptional Audio
- Connectivity Options
- Enhanced Worker Safety
- Enhanced User Experience
- Built Tait Tough

TOUGHER, SMARTER, SAFER COMMUNICATIONS

You’ve got options.

Learn more about the new **Tait Tough** range at **www.taitradio.com**

TAIT TOUGH
The Toughest Radios in the Industry

US public safety LTE networks

The USA is undertaking a major project to build a nationwide public safety broadband network using a commercial provider, but it faces some unique challenges in realising its ambitions, as **James Atkinson** reports

The USA is at the forefront of nations pioneering the migration of public safety agencies from narrowband land mobile radio (LMR) wireless communication platforms to broadband LTE systems.

In 2012, Congress passed legislation to build the first-ever Nationwide Public Safety Broadband Network (NPSBN) and set up the independent First Responder Network Authority (FirstNet) to oversee its implementation and operation, along with granting $7bn in funding.

Mobile carrier AT&T was awarded a 25-year, $6.5bn contract to build and maintain the public safety network in March 2017 and was granted 2 x 10MHz of 700MHz (Band 14) spectrum for both public safety and non-public safety use to complement its existing 4G LTE spectrum holdings. AT&T is providing FirstNet access to its infrastructure and is spending $40bn to maintain and improve its network.

Unlike its fellow mission-critical (MC) LTE public safety network pioneers in the UK and South Korea, the USA faces some unique challenges, not least of which is its sheer size. Implementing the ubiquitous coverage that first-responders require across all its vast states and territories is a tall order and an expensive one compared with the geographically much smaller UK and South Korea.

And then there are the high numbers of first-responders that need to be migrated. There are upwards of 60,000 public safety agencies in the USA and more than 10,000 LMR networks. Rough figures estimate there are between 750,000 and 850,000 sworn police officers, 826,000 licensed and credentialed Emergency Medical Services (EMS) professionals and around 1,216,600 career and volunteer firefighters.

The other catch, and it is a very significant one, is that although all 56 states and territories have allowed FirstNet/AT&T to deploy the network in their states, there is no requirement for state and local public safety agencies to use the network. AT&T must attract users to the network to ensure it is self-sustaining, as required under the legislation. But other mobile carriers, Verizon in particular, are offering similar services, which may affect FirstNet/AT&T's enrolment efforts.

Other factors affect enrolment. Some public safety agencies have expressed reluctance to join FirstNet, citing uncertainties with the resiliency, reliability and security of the network, coverage and cost. Others want to wait until they can access the mission-critical voice services they are used to on LMR networks.

The sheer size of the USA is just one of the major challenges the country faces in rolling out nationwide public safety broadband coverage

Coverage

Ryan Poltermann, innovation architect at Commdex and vice-chair, LMR-LTE Integration and Interoperability Working Group of the National Public Safety Telecommunications Council (NPSTC) – an organisation of 15 public safety organisations, along with federal, state and local government representatives – believes that coverage is the main influencer of choice.

"In the US, coverage remains the factor for selecting a carrier. This coverage issue may preclude one or more carriers from even being a choice to public agencies, and it is worth mentioning there are biases that would prevent switching even if the coverage were equivalent or better," says Poltermann.

AT&T currently offers an Enhanced PTT service from Motorola Solutions' Kodiak Networks and says it will provide a 3GPP-compliant mission-critical push-to-talk (MCPTT) service in early 2020. It has also selected a second MCPTT provider, but has not yet revealed who this is.

Adobe Stock/Gorodenkoff

"This is a standards-compliant, mission-centric solution that's being purpose built for public safety," says an AT&T spokesperson. "It's designed to further advance first-responders' communication capabilities with reliable, high-performance calling. We'll have more to share in the coming weeks and months."

AT&T's main rival Verizon has not taken this lying down and is busy competing for public safety agency subscriptions by also offering priority and pre-emption voice and data services. It also offers Motorola's Kodiak Networks carrier-integrated PTT service, as well as a variety of over-the-top (OTT) PTT service providers such as ESChat. Sprint also offers Kodiak.

T-Mobile has said that if its proposed merger with Sprint is finally approved, it will offer free 5G services (once it has rolled out a 5G network) to first-responders through its Connecting Heroes Initiative. It has not stated whether priority and pre-emption services will be available or if it intends to offer a 3GPP-compliant MCPTT service.

This provides a scenario where four (or three) carriers are, or will be, offering MCPTT, carrier-integrated PTT and OTT PTT services. Plenty of choice for public safety agencies, then. Some see this multiplicity of choice as a good thing as it ensures competition; others think it dilutes the FirstNet ideal of a single, nationwide mission-critical network for all first-responders.

"I believe we should expect multiple vendors providing Release 13-compliant MCPTT solutions in 2020 in the US," says TJ Kennedy, former president of FirstNet and now one of the co-founders and principals of The Public Safety Network consultancy. "I am excited to see a competitive marketplace."

However, Poltermann worries that this multiplicity of choice may have consequences for the public safety community. "We face distinct challenges that other nations won't have. Because of the lack of an integrated approach, the agencies are free to choose whichever communications method they wish. This causes issues not only for interoperability, but also from a collective bargaining standpoint. This lack of collective bargaining means that the features public safety desires may not be received."

Certainly, FirstNet/AT&T will need to offer a more attractive service if it is to succeed in its ambitions and stave off competition from other rivals. A FirstNet spokesperson says: "FirstNet is driving innovation in the public safety broadband marketplace in the United States. The network is driving competition and choice, and delivering dedicated public safety services like pre-emption that did not exist before FirstNet.

"We worked hand-in-hand with the public safety community in all 56 states and US territories to understand their coverage and capacity needs for the network. This is unique to FirstNet." And as the spokesperson points out, it is still early days. FirstNet is just "two years into a five-year deployment based on individualised state buildout plans, and AT&T continues to be ahead of schedule".

Kennedy says: "The speed at which this has been delivered across the country has exceeded expectations. It is an opportunity to leverage open standard solutions to create true operability for all public safety communications by leveraging MCPTT/Data/Video."

> I believe we should expect multiple vendors providing Release 13-compliant MCPTT solutions in 2020 in the US

Interoperability

Interoperability, or operability, as Kennedy prefers to call it, is critical. FirstNet was largely conceived because of the interoperability issues faced by public safety agencies responding to the 9/11 attacks when their different LMR networks were unable to communicate with each other.

But what does interoperability mean here? Does it mean the MCPTT, carrier-integrated PTT and OTT PTT options available on AT&T should be interoperable with each other? Or that the MCPTT and OTT PTT services offered by other carriers should be interoperable with AT&T's FirstNet service: ie, have access to the FirstNet secure core?

This is what lies at the heart of the Boulder Regional Emergency Telephone Service Authority (BRETSA) petition to the FCC, which has attracted support from other jurisdictions, as well as Verizon among others. BRETSA wants the FCC to make a declaratory ruling that FirstNet/AT&T should provide access to the FirstNet core to ensure operability between all first-responders who have chosen another provider and want the freedom to continue to do so. FirstNet and AT&T oppose this and want the petitions dismissed.

Kennedy observes that in the FirstNet model, the RFP required multiple mission-critical PTT solutions to be made available on FirstNet and to ensure there was full operability across those solutions. "This is an important element which means that the MCPTT solutions running on FirstNet will be tested and operable with each other. This also provides competition for MCPTT services on FirstNet and will drive innovation and competitive pricing." If this is the case then that will ensure operability between PTT

▸

Adobe Stock/csfotoimages

solutions on FirstNet, but it does not ensure operability between carriers.

"It is in the interest of public safety to have interoperability," says Poltermann. "While I am of the mind that having all users on one network makes things a lot easier and safer, the reality is that there's multiple networks. Multiple carriers with interoperability using open standards and allowing for flexibility in UE and applications is best for US public safety." Hence he wrote in support of BRETSA. But he is concerned that the cheaper OTT PTT clients are a significant threat to the take-up of MCPTT.

"There's a lot of unknowns about implementation," he says. "We currently face interoperability issues on the current carrier PTT platforms based on the 'customer'. If one agency pays for a device and another one pays for the other, they can't talk to each other through PTT. We're worried about it rippling into MCPTT."

Kennedy is more optimistic and thinks the superior service MCPTT will offer will ensure a good take-up. "I believe MCPTT will be successful since it will meet all the functional demands being met by P25 today for most departments. Open standard solutions are important."

Ken Rehbehn, directing analyst, critical communications at Omdia (IHS Markit), argues that data services on LTE have some important differences that make the interoperability question less pressing. "First, by moving to LTE we automatically gain an interoperable environment thanks to the 3GPP protocol set. The degree of connectedness then becomes a political, not a technical, question.

"More fundamentally, unlike past voice systems, the data system of 3GPP underpins access to the cloud, which is by its nature completely interoperable thanks to standardised web interfaces. This diminishes the argument about interoperability, but it does not eliminate it entirely. If the cloud is isolated in a walled-off portion of the internet, interoperability becomes a question of cloud access instead of radio access.

"The FirstNet core, for example, is largely isolated from the broader internet. A PTT voice solution hosted on FirstNet core will, as a result, not be interoperable to users without access to the FirstNet core. So, the problem is mainly political, but there is still a potential trace of the technical interoperability issue," says Rehbehn.

If public safety agencies use other mobile operators besides FirstNet/AT&T then it will be necessary to ensure interoperability between carriers to allow different agencies to communicate with each other at major incidents – the issue is largely political and commercial, rather than technical

MC LTE at scale

Where Rehbehn sees a potential problem in the future is with the transition to MCPTT over LTE at scale, as this will require LTE network broadcast capability – 3GPP Evolved Multimedia Broadcast Multicast Services (eMBMS).

"We need eMBMS to enable very large talk group communities. Broadcast eliminates thousands of redundant voice packets arriving at handsets at different times. Without eMBMS, we cannot achieve MCPTT scale. The issue there is that broadcast mechanisms are poorly defined for operation across network boundaries," he says.

The danger is each network becomes an island and agencies on FirstNet for MCPTT and others on Verizon or T-Mobile are not able to communicate during a major incident. "That brings us back to a very bad starting point, and prevents wholesale fleet migration to MCPTT," says Rehbehn. "In my opinion, the missing eMBMS features will ultimately force all public safety agencies in the US to move to FirstNet or remain on classical Project 25 systems forever."

This brings us to the crux of the matter behind the BRETSA petitions, because as Rehbehn points out: "For FirstNet, there is a commercial imperative to not fix this eMBMS limitation. This issue is not a technical problem, it is a commercial one. AT&T is a business and it potentially has a captive audience, so why would it risk losing them to a competitor by opening up [a] hole in the wall allowing other carriers with first-responder subscribers to access its FirstNet core and services?"

Direct mode

A further challenge to the migration to MC LTE services, and one that faces every country looking to follow suit, is the lack of an adequate direct mode, radio-to-radio solution in 3GPP – Proximity Services (ProSe) or Sidelink, as 3GPP calls it.

As Poltermann points out, the coverage between a P25 site and a cellular site is distinctly different (particularly P25 on VHF). "The overall coverage issue also comes into play with ProSe/Sidelink, because there are large areas of the country with inadequate coverage. We're a bit concerned about ProSe, and we'll have to see how it plays out."

Rehbehn goes further, saying: "The lack of a viable direct mode/ProSe solution for MC LTE stands as the biggest barrier to wholesale fleet migration to MCPTT." While the current 3GPP ProSe might be adequate for outdoor direct mode, Rehbehn is doubtful it will be powerful enough to provide indoor-to-outdoor connectivity. In addition, ProSe has had little support from silicon vendors, with only Samsung saying it will implement it.

Alternatives involve either pairing LTE devices with some form of other device to provide direct mode services, or integrating two radios into a single device. Rehbehn says: "L3 Harris has made some interesting developments here, combining LMR and LTE in cost-effective general purpose radios for both vehicles and handheld devices."

Poltermann says this makes carrier support for interworking between LMR and LTE extremely important. 3GPP has completed its work on the interworking function (IWF) in Release 16, but ATIS/TIA in the US are still working on how to implement it in P25 systems. "We'll have to see just how many vendors implement it," says Poltermann. "The ripple-down requirements means that it will take some time to appear."

Public safety agency engagement

One disadvantage AT&T faces is that it is subject to oversight and public scrutiny in a way that Verizon, T-Mobile and Sprint are not. It also has the weight of the public safety community's expectations to contend with, and it seems this might need some attention.

Poltermann observes: "FirstNet's strategy is not particularly clear. While a roadmap has been published, the roadmaps don't provide timelines or even solid goals. To be a little harsh, FirstNet communication throughout the whole process has been rather terrible."

Rehbehn points out that FirstNet is locked into a very long-term contract with AT&T with confidential terms and conditions. "Unfortunately, the

▸

FirstNet: Progress so far

AT&T began work on building the Nationwide Public Safety Broadband Network (NPSBN) in 2018. This involved building a separate secure network core for FirstNet, which provides priority and pre-emption services to FirstNet subscribers. It continues to build out its Band 14 700MHz coverage sites across the country. The roll-out is ahead of schedule and was about 75 per cent complete in January 2020.

AT&T has not revealed the number of vehicular connections versus people or what proportion of them are primary or secondary responders, but it reports that "more than 10,000 public safety agencies and organisations across the country have subscribed. And over one million FirstNet connections are in service. Current users span federal, state, local and tribal public safety agencies of all sizes, as well as an extended community of users that can be called on to help support first-responders."

Public safety agencies using FirstNet have access to a nationwide, dedicated fleet of 76 land-based and airborne portable cell sites. Stationed across the country, these assets are available 24/7 at no additional charge to FirstNet subscribers to provide additional connectivity in support of public safety's mission. During 2019, the FirstNet Response Operations Group fielded more than 450 requests for additional planned and emergency support.

An AT&T spokesperson says: "FirstNet is spurring innovation with more than 100 FirstNet Ready devices and a catalogue of over 100 apps specifically certified for public safety that can help cost-effectively increase first-responders' capabilities and situational awareness."

Mission-critical networks need to be 'hardened' to withstand power failure and environmental damage. The AT&T spokesperson says: "We're rebuilding with network-hardening materials – when possible, we're deploying hardened antennas that can withstand hurricane winds, fibre with reinforced cores, and steel hurricane poles versus wood for attaching fibre; during [Hurricane] Maria, we tallied the much higher rate of steel poles withstanding winds versus wood poles that snapped.

"We carefully assess each disaster rebuild – whenever possible, we move networks to updated facilities or to a newer technical solution, such as copper to fibre. We trench and bury new facilities where possible. Unless a like-for-like solution is better for the customer for faster restoration, we look to upgrade. For example, in the recent 2019 Dallas tornadoes, areas where we had already built fibre to impacted neighbourhoods, we moved customers on copper over to the new, more reliable fibre service whenever possible."

In terms of indoor coverage, the AT&T spokesperson says: "FirstNet gives public safety access to more than 6,000 existing AT&T in-building assets. This includes in-building solutions in place at stadiums and transportation facilities.

"Plus, Band 14 provides good propagation in urban and rural areas, penetrating buildings and walls easily and covering larger geographic areas with less infrastructure. Only FirstNet subscribers can obtain always-on priority access to and, for primary users, pre-emption on, Band 14 – no other wireless provider can do this."

AT&T has an advantage over its rivals as it can operate high-power user equipment (HPUE) on its Band 14 spectrum to extend coverage range.

opaqueness of the contract between FirstNet and AT&T does not help agencies gain confidence. We do not know what the KPIs are or how AT&T is stacking up."

A Government Accountability Office (GAO) report published in January 2020 tends to agree. While GAO found that AT&T was on track or ahead of its milestones, it suggested that FirstNet needed to tighten up its oversight and be more transparent. It also noted that public safety officials "were dissatisfied with the level or quality of information received from FirstNet" as regards AT&T's progress or FirstNet's oversight. GAO also thought FirstNet could do more to try and gauge end-user satisfaction.

FirstNet is not contractually obliged to share such information, but GAO pointed out that key practices call for communicating appropriate information to relevant stakeholders and reporting on monitoring results. Sharing more information about the oversight FirstNet conducts could improve public safety stakeholder sentiment for and support of the programme, it stated.

In response to this, the FirstNet spokesperson says: "The FirstNet Authority has accepted the GAO's recommendations to further enhance the FirstNet Authority's contract oversight and stakeholder outreach processes and is currently working to implement them as part of our public safety engagement programme."

Next steps

Looking ahead at how things might develop, Kennedy says: "I predict most public safety agencies in the US will start to transition to MCPTT in 2020 and most others will add it no later than 2021. I see MCData and MCVideo naturally following on next. It will be the de facto standard for public safety to communicate across LTE.

"There will be significant focus on situational awareness tools and integration as well as user experience in 2020. You will also see MCPTT and more integration with other PTT systems in 2020."

In 2020, the first 3GPP-compliant mission-critical push-to-talk services are due to be launched, which should provide public safety agencies with access to improved MC services

However, other agencies are still purchasing P25 systems, and as Poltermann points out, they are expensive. "This amount of investment means there's an expectation of using the devices as long as possible. There will be a transition period of course, but for the US it could be a decade or two."

Nonetheless, as the AT&T spokesperson says: "FirstNet represents an unprecedented public-private investment in infrastructure that makes America a leader and public safety a national priority."

This is undoubtedly true, but if the political and commercial realities of the US market mean public safety agencies continue to use different carriers for MCPTT then a solution to the current interoperability stand-off between FirstNet/AT&T and other providers will need to be resolved.

Adobe Stock/lufeethebear

Cameras that have brains as well as eyes

Facial recognition technologies are increasingly being used by the public safety community, particularly for law enforcement, but they are proving controversial. **Charlotte Hathway** finds out whether this criticism is proportional

Technologies that accelerate public safety tasks and processes can transform outcomes for those affected by the issue being addressed. Yet new technologies often create new questions for everyone with a stake in that issue. Few emerging technologies, at least in recent years, have been met with the uneasiness that has followed facial recognition trials and roll-outs. This has created an environment of distrust between citizens and those tasked with protecting them.

Dame Cressida Dick, commissioner of London's Metropolitan Police Service, recently said that "inaccurate" critics should "justify to the victims of those crimes why police should not be allowed to use tech… to catch criminals" in response to a Royal United Services Institute report that called for tighter rules on police use of technology. A month prior to those comments, the Metropolitan Police Service announced it will begin the operational use of Live Facial Recognition (LFR) technology developed by NEC, a Japanese technology company. Those comments seem to have been intended to alleviate distrust of this technology, yet the reader will likely either welcome or reject that explanation based on their existing views on facial recognition.

It can be difficult to sort the facts from the fiction – from the current capabilities and near-term developments, through to the regulatory landscape surrounding its use. The public safety community is known for its cautious use of new technologies – is this new territory any different?

Current capabilities

NXP Semiconductors develops the components that power facial-recognition technologies. Microcontrollers, processors and sensors like those produced by NXP are foundational to enabling facial and object recognition due to the data analytics and multiple-protocol communications carried out by these components. Steve Tateosian, senior director for IoT and security solutions at NXP, explains that NXP participates ▸

in the production of facial recognition technologies from a technology perspective in three different ways: providing its processors to developers; providing tools, software libraries and a software development environment to enable developers to more easily develop facial recognition applications; and providing a complete facial recognition solution (including software and hardware).

Tateosian adds: "In some of our newer devices, there are hardware accelerators that are specifically designed to accelerate neural networks and our software development environment, called eIQ, enables developers to take a wide variety of models and inference engines and port those in an efficient way to NXP processors."

NXP has just launched a new 'vision solution' that includes a hardware module design and associated software to facilitate offline face and expression recognition. This means, Tateosian explains, "a customer can buy a module with a camera on it and the second they plug it in, they can see their face through the camera and see that it's not recognising their face. Then we have a set of different ways that they can train faces on the device, instantly."

This simplification of the development cycles behind facial recognition technologies opens the doors to more widescale use in the coming years. Tateosian says: "What used to require very high-performance processors and cloud-based support for processing can now be done on the edge without cloud intervention. The devices themselves are changing, of course, but really the bigger breakthrough is on the software side. The software is getting more and more sophisticated and streamlined, and that is enabling face recognition to become more prevalent in the future.

"There's always – or maybe I'm overstepping to say 'always' – but there's always going to be this use-case for really sophisticated, cloud-based facial recognition for public security or through customs or immigration and other areas. There may be these powerful engines that can recognise multiple faces at a single time and process those in the cloud."

He adds: "Being able to do all the processing and learning on the edge means the devices themselves don't need to be connected to the cloud and any faces that are registered on the device can simply be erased by the user." This capability might help lower citizen discomfort with facial recognition technologies being used by law enforcement in public spaces. Products like those developed by NXP mean the device "doesn't ever need to send the face ID information to the cloud. All the facial data and the camera feed remains local on the device itself."

NXP says its facial recognition portfolio is powered by an 'interference engine'. Tateosian says this term is used to explain the processing that takes place on the device itself. He explains that these engines are created based on a large dataset and, for vision, the first thing the camera needs to do is find the head in the frame. The interference engine is used to find the face in the frame of the image and then focuses on the face and creates a model that can be pushed through the engine to see if there is a match on the other side.

Understanding the limits

Facial recognition falls under a broader category of biometric data. Yet other types of biometric data do not have a similar perception of inaccuracy. Merritt Maxim, vice-president and research director at Forrester, explains that fingerprints have a long history of research, and fingerprint analysis is supported by intellectual property that is accepted as highly accurate. He says: "Fingerprints have been used for decades, so there is a good understanding of how it works and how fingerprints can change. Facial recognition is much newer and therefore hasn't had the same level of usage in the field and that's why there continues to be questions about how well it adapts to behavioural changes. You get older, your hair gets gray, you grow a beard, or you get wrinkles or other things… does a facial recognition technology have the ability to adapt to those physiological changes and still maintain a high level of accuracy?"

> "The bigger issue is the inherent biases that seem to exist in some facial recognition algorithms"

That question, Maxim says, will not be answered in the near term. He says: "We won't really know until this has been used for an extended period of time. Right now, we're still in the early stages. What I looked like 10 years ago is a little bit different to what I look like now. Can facial recognition adjust? Until we see that in reality, I think that's still an open question."

Maxim adds: "The bigger issue is some of the inherent biases that seem to exist in some facial recognition algorithms, with strong racial or gender biases that mean people are misidentified. Some of that can be based on the data that's used to train the model, and that can potentially lead to the apprehension of the wrong individual because the facial recognition technology didn't make the correct match."

This does not sound like an easy issue to iron out. When asked whether technology companies or public safety agencies will need to build new datasets that are representative of the population being observed, Maxim said he believes how this will play out is to be determined. More diverse sets of training data would of course help, but other functionalities or capabilities might emerge that also help deal with the issue of bias.

A need to improve the accuracy of these technologies is also an area identified by NXP's Tateosian. He says: "I think there's going to be more and more improvement both in the fundamental technology and doing so under different conditions. Lighting conditions, for example, have a large role to play in this. Being able to maintain accuracy across a wide range of lighting conditions is important, and I think that's something that's going to happen."

Tateosian also anticipates the systems running facial recognition algorithms to develop in a way that means they require lower power. This "means you're going to start to see these things in battery-operated devices as well".

Existing functionalities will also gradually reduce in cost, which will make them more accessible to a wider range of applications. Those include emotion detection, age prediction and gender prediction, and Tateosian says they are "really on the high end but I think you're going to see them become more mainstream".

There are also various studies that demonstrate facial-recognition software can be tricked. In February, software company trinamiX shared details about its 'skin-detection' technology – an alternative that it says can detect the material it is analysing. This prevents masks, for example, from hiding someone's identity. It remains to be seen whether that modification will become widespread.

The regulatory puzzle

The regulatory landscape around the use of this technology is complex and varies around the world. It is not possible to delve into these intricacies in one article.

In the UK, an interim report of the Biometrics and Forensics Ethics Group's Facial Recognition Working Group was published in February 2019. It was a response to live facial recognition (LFR) trials undertaken by South Wales Police and the Metropolitan Police Service. The report found that there is a lack of independent oversight and governance of the use of LFR. It recommended that police trials of LFR should comply with usual standards of experimental trials until a legislative framework is developed. Given the Met Police has moved ahead with operational use of LFR, it is clear the report needs to be updated. A secretary for the working group advised that a further report, in collaboration between police forces and private entities, is expected this summer.

Then, in October 2019, Elizabeth Denham, the UK information commissioner, published a blog that made her feelings clear – "police forces need to slow down and justify its use". The Information Commissioner's Office (ICO) is the UK's independent regulator for data protection and information rights law; it has specific responsibilities set out in the Data Protection Act 2018 and under the General Data Protection Regulation (GDPR).

The ICO carried out its own research to understand the thoughts of UK citizens, and found there is strong public support for the use of LFR for law enforcement purposes – some 72 per cent of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime. Denham links to that research in her blog, so presents a balanced approach to this technology. The ICO is not trying to prevent its use, it is saying it needs to be used cautiously.

Denham said: "Moving too quickly to deploy technologies that can be overly invasive in people's lawful daily lives risks damaging trust not only in the technology, but in the fundamental model of policing by consent. We must all work together to protect and enhance that consensus."

The following day, Tony Porter, the independent surveillance camera commissioner, added to the ICO's findings. Porter said that the use of automatic facial recognition (AFR) should be within the confines of existing regulatory guidelines. He pointed to a recent Cardiff judgment that clearly set out the Surveillance Camera Code of Practice (SC Code) and section 33 of the Protection of Freedoms Act 2012 as key elements of the legal framework for the use of AFR.

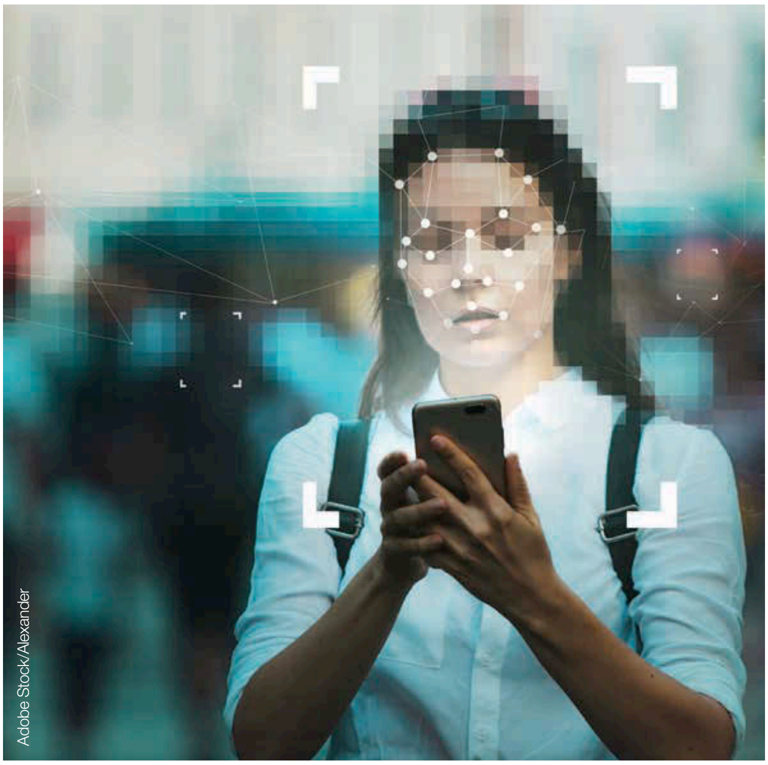
While that ruling found that South Wales Police's use of facial recognition was proportionate, it made clear that the force should be prepared to demonstrate its use is justified according to the particular facts of individual cases. This means that facial recognition should not be used without clear justification.

In the US, the regulatory landscape is even more fractured. Forrester's Maxim points to various examples of state-level regulations, starting in Illinois in 2008 with the Biometric Information Privacy Act (BIPA). He says these regulations "reflect the growing interest and concern around facial recognition". The political landscape in the US means that "no two laws will necessarily be written exactly the same way, so it does create some real challenges if you are a national organisation trying to deal with this growing patchwork of biometric laws. In the European case, GDPR is providing a more holistic view, but certainly here in the US, this continues to be a real problem and probably is not going to get any better because there's really no real momentum or interest in a national equivalent of GDPR right now. That means [regulations are] going to be at the state or local level for the time being, unfortunately."

What is interesting about that BIPA law, explains Maxim, is that it "was written well before touch ID or face ID even existed, yet it provides protections and consent if you are collecting biometric data. There have been, in the last year, several court cases against organisations that have potentially violated the spirit of that law. [Various courts have] ruled against organisations that [have been] collecting [biometric] data. This is a law that gives some consumers some protection and means to challenge what's happening and potentially get some relief out of the misuse or miscollection of data over a period of time."

Last summer, Somerville, Massachusetts became the second US city to bar municipal use of facial-recognition technology due to ethical concerns including the potential for government misuse and its unequal performance across racial and gender lines. At the time, Maxim explains that, ▸

Although most of the public support the usage of facial recognition for law enforcement, those employing it must still justify its use in order to assuage the tech's critics



Adobe Stock/Alexander

despite these new limits, he expected the technology to survive scattered bans by state and local governments. He says: "The technology's already been developed, it's already being deployed for a range of different use-cases. It'll continue, definitely."

One reason why facial recognition might have attracted such controversy is because it is easier for data to be covertly collected compared with other types of biometric data. Forrester agrees with this hypothesis. He explains: "It's non-invasive. In the case of fingerprints, you need to physically present your hand or finger to a sensor to collect that data, whereas facial ID data just needs a camera and then it can start collecting images of people without any consent at all."

In December, cyber-security firm Comparitech published a study looking at how extensively and invasively biometric ID and surveillance systems are being deployed. It ranked 50 countries and found China uses facial recognition technologies more extensively than any other country surveyed, including the introduction of a new facial recognition check for anyone getting a new mobile phone number. It also found China does not have "a specific law to protect citizens' biometrics".

What facial recognition technology should be used for clearly varies across borders, yet not all perceptions of facial recognition are negative. Maxim explains: "Fingerprints are, for a lot of people, very closely affiliated with criminal activity in a sense that when people are arrested on TV or in movies, they are usually fingerprinted. And that fingerprint goes into the criminal record. So if an organisation is asking for your fingerprint, people often have a negative opinion because they think of it as a technology that's used more for a criminal scenario. Facial recognition doesn't have that stigma attached to it. That stigma might be unfounded, but it does persist. That also has influenced consumers' perception and willingness to have their fingerprints collected."

> "Moving too quickly risks damaging trust not only in the technology, but in the fundamental model of policing by consent"

Optimistic caution

New technologies are never perfect. That is why initial implementations should tread cautiously, using the information provided as a guide, not an instruction. There is no evidence that facial recognition is yet being used in any other way than that.

More work is needed to improve the accuracy of the algorithms, and gender or racial biases must be taken into account. Law enforcement agencies should be as transparent as possible, to help reassure citizens that this technology is being used carefully and proportionally. Fingerprints have been vital in law enforcement activities, and citizens now expect these to be collected. Facial recognition, as just another type of biometric data, could eventually be thought of in the same vein, if the information is taken at face value – something that is informative but imperfect. Research and development will help improve that accuracy, we aren't quite there yet.

Adobe Stock/alice_photo

Network resilience and redundancy planning

Private PMR public safety networks are designed to be highly resilient, but the migration of critical communications users onto commercial 4G networks increases the complexity of planning for resilience. **Richard Martin** looks at how it can be achieved

Public safety networks need to be resilient during man-made problems, from the digging up of a cable to a major natural disaster such as an earthquake. In the latter case, this will be exactly the time the service is most needed. Planning for and building network resilience is vital if the service is to meet its objectives and keep the general public and emergency services safe and effective.

Resilience measures can be implemented in all parts of the radio network, including its primary elements, power supply, links redundancy and switching back-up solutions. Such measures are commonly found in PMR networks, but now 'best effort' commercial 4G/LTE networks looking to host mission-critical communications users are having to step up to meet these users' more exacting requirements.

Base station resilience and backhaul

Kevin Humphries, market specialist – TETRA infrastructure at Motorola Solutions, has been involved in numerous TETRA projects around the world. Starting with power supply, he says: "We have been using a range of solutions for power, either as back-up for mains or as alternatives. Battery back-up is common on conventional sites, but we have provided diesel generators on remote sites where mains is not available.

"In the Middle East we have provided a combined solar and battery combination, and have seen some customers use oil or natural gas generators along pipelines with a feed of fuel from the pipeline itself. I am also aware of a hydroelectric-powered base station in Iceland. In Norway, we have used hydrogen fuel cells. These are an eco-friendly solution, but expensive."

How much back-up time should be provisioned with batteries? "That depends, it relates to the importance of the site. For example, is it the only one in the area? Also, its accessibility – is it difficult to reach to replace batteries or deploy a temporary generator? In some cases, it may be necessary to provision months or even a year of fuel if the

Continuity of power supply is a key resilience measure; batteries, diesel generators and solar power are all used for failover power generation site is very remote, although in the Middle East we have seen a weekly replenishment commonly."

In terms of security, Humphries adds: "Perimeter security can be enhanced with IR sensors and CCTV cameras, and it is also helpful to have CCTV in the shelter to see who has access to the cabinets. Alarms on doors or fences and gates can alert network managers to unauthorised ingress."

Vicente Rubiella, product manager – systems, NEBULA TETRA Infrastructure at Teltronic, adds: "Back-up power-generation types will depend on the customer preferences and terrain characteristics. For example, solar panels can be a good option for isolated areas where grid connection is impractical or involves an unreasonable cost. Back-up power-generation equipment must be dimensioned accordingly to provide power throughout the expected time to restore the primary power source in case of failure, usually 24 hours."

Jochen Boesch, senior director, engineering at Damm Cellular Systems in Denmark, states: "Typically -48Vdc is used to power base stations. This allows for generator, batteries and solar panels in parallel usage. Our base stations also offer 230Vac input to use a UPS."

Humphries says: "Critical sites should have duplicate links, perhaps from different suppliers. Different technologies can come into play here. If two separate fibre or wire links cannot be provisioned then a microwave or satellite link may be used. Remote sites may only be able to use satellites; good practice would be to connect through two different satellites. 4G gives us another link as a back-up."

> "When a master fails, the system will automatically make a slave node the master"

Opinions differ on the merits of centralised and decentralised network architectures, but measures can be implemented to make both highly resilient

Switch and core

There are different approaches to centralised or distributed switching. Motorola Solutions favours centralised switches. It cites the reduced traffic between the Zone Controller which tracks all base stations, compared with a distributed system where all base stations need to negotiate and pass call information to each other.

This zone controller also knows where every radio and group are located and only sets up calls on base stations where users are present. In terms of resilience, services are maintained if there are local failures. Humphries adds: "Although centralised, our systems provide duplicate processors and there can also be mirrored processors in different locations to provide geographical redundancy. Regional centres such as the counties in the UK can take over the control in another county in the event of a major failure."

Boesch from Damm makes the case for distributed switching. "Distributed networks can keep a full feature set if a subset of nodes become isolated, and are easily scalable with new sites added without increasing switch capacity. As well as quicker set-up times for local calls, the backbone traffic can match or better a centralised switch if set up intelligently. A master/slave concept for back-up in a decentralised system is easy to handle. When a master fails, the system will automatically make a slave node the master – the same also goes for applications connected to gateways."

Teltronic advocates centralised switching. Asked whether this is less resilient than distributed, Rubiella states: "Definitely not. Centralised architectures provide all kinds of facilities to feature the highest level of resiliency, when redundancy is vital. Having a centralised switch and a hot standby back-up switch, where no user action is needed to perform an immediate switchover on detection of failure condition, achieves the most resilient network deployments in a cost-effective way."

Regarding failover mechanisms, Rubiella concludes: "Failover must rely on two basic and essential requirements: rapid detection of failure condition to trigger switchover immediately; and no user action needed, but automatic switchover between main and back-up unit."

This debate will continue. Potential users would be wise to carefully compare offerings from several suppliers to make the best decision for themselves and their particular needs.

LTE joins the club

The introduction of mission-critical specifications into 3GPP 4G and now 5G means cellular network operators also have to consider higher levels of resilience. With the 3GPP Releases 12-14, public safety features were added to the LTE standard including Proximity Services. This becomes a resilience feature in that users can still be connected when access to a base station is no longer possible. In addition, the QCI (Quality of service Class Identifier) features enable preferential access for critical users when public LTE service is also used. Base stations can also work in isolated mode if all links are down.

Stephane Daeuble, head of marketing – enterprise solutions at Nokia, and Hansen Chan, its product marketing manager, outline some of the resilience features in LTE. Daeuble observes: "The normal resilience level for a private LTE system is 99.9 per cent, but this can be easily increased to four nines or higher, with dual connectivity (using two different frequency layers) to base stations, and reserve power. Also, by using two different frequencies, users are connected to both frequencies at the same time and this will bring availability up to 99.999 per cent. Looking at base station availability, much lower power consumption has made it easier to run on alternative power sources such as batteries or solar panels."

Nokia has moved to greater levels of silicon integration and increased power amplifier efficiency, meaning that a small cell with RF level equivalent to a macro base station can be run on 90-200W, giving a radius of operation of over 90km with the right antennas and deployment height. Miniaturisation has also enabled the development of portable base stations, which can be deployed in an emergency or network failure.

A helicopter could transport an operator with a rucksack-sized base transceiver station (BTS) to provide coverage over several kilometres radius, making for a completely standalone system for a major emergency. The later addition of a satellite link allows this standalone network to connect to the internet or a wider network to enable communication between the team in the field and people in response centres.

This size reduction also makes it possible to have a base station on a drone, which could be tethered to a vehicle to maintain power nearly indefinitely. Balloon-mounted small-cell BTSs could work for several days typically, versus hours with older generation macro BTS.

Asked whether LTE networks can backhaul themselves, Daeuble responds: "With frequencies being a precious resource, I would say that it is better to use other technologies such as fibre or microwave or unlicensed frequencies for reserve links for base stations."

Expanding on the switching and core aspects, Daeuble and Chan say: "Regarding the core, our default is two cores or blades, but you can also enhance this with geographical redundancy and even use the core of the public mobile service when possible as the third level of resilience. It's important to have procedures in place to control when switch back-up is initialised.

"There can be a constant monitoring of the network end-to-end by heartbeat messages through the backhaul network between the base station and the core, then automatic switching if a failure occurs. But there is a case for manual intervention if it is felt that approvals would be needed before switching takes place. Last but not least, the backhaul network also needs to be resilient."

As regards 5G in public safety, Daeuble and Chan add: "5G with new radio (NR) and core (SA) will offer very

▸

Real-world MC LTE implementations

The UK and the USA are both actively moving to an LTE-based public safety communications system, with some differences. In the UK, EE is the provider of the network under contract to the government. It has described how additional resilience is being built into both the core and radio networks.

An EE spokesperson says: "EE have already demonstrated the core network's high level of resiliency to the emergency services. This is delivered through geographic separation and redundancy of switches and servers in each core node. 4G sites are typically closer together than TETRA sites, primarily for capacity, but this overlapping coverage adds to the network's resilience. Many more EE sites now have transmission resilience, with diverse fibre routing, microwave back-up or satellite back-up."

Power resilience is addressed through battery power supplies, permanent or portable generators, ensuring continuity for key sites. "EE's Business Continuity & Disaster Recovery Plans have been designed, implemented and tested around robust ITIL-based Service Management Frameworks to meet demanding performance measures.

"Our mobile base stations and rapid response vehicles can be deployed quickly to restore coverage in the case of a total site failure (such as road traffic accidents or arson attacks) and portable satellite backhaul can quickly get sites back online if transmission is damaged. The emergency services get priority access to the EE 4G network as per GSMA standards, enabling connections even in highly congested sites."

EE claims that this range of measures has proven to be successful in preventing outages during extreme weather events and power cuts.

In the case of the USA, a First Responder Network Authority (FirstNet) representative states: "We worked hand-in-hand with first-responders across the United States to understand their critical communications needs for a public safety LTE network. They emphasised the importance of resilience and redundancy to ensuring the availability of the network, and the FirstNet Authority outlined them as objectives in our Request for Proposal for the network.

"Public safety also identified that having a dedicated set of deployable assets was vital to emergency response, and we have seen much success to date with the FirstNet deployable fleet (including blimp below). High Power User Equipment (HPUE) is another potential tool to help increase the effective range of cell sites at the edge of the network. AT&T plans to test and roll out HPUEs for FirstNet subscribers which are only authorised for use in FirstNet's Band 14 spectrum."

high bandwidth for data, increased reliability and low latency features that will come as the 5G standard matures with Release 16-17 and 18. In addition, with slicing capabilities, 5G will also mean that mobile operators can offer a designated resilient service with guaranteed quality of service for public safety use over their public networks.

"But slicing services will also require mobile operators to expand the coverage of their 5G network currently limited to major cities. These kind of capabilities brought by the new 5G standards will come during 2021-2023, and devices that support these features a few years after."

Boesch from Damm observes: "Do public safety users need to have separate cores? Many vendors do offer IP applications running on smartphones that can get tunnelled and encrypted/authenticated through any kind of IP backbone to connect to the secured centralised or decentralised core."

Raquel Frisa, product manager – systems, LTE and Command & Control at Teltronic, takes a different view on separate cores in a 4G network. "The use of a separate network core is essential to guarantee the reliability in broadband networks. But this is not the only requirement when the public agency needs to deliver mission-critical (MC) services. In fact, our recommendation also involves the use of dedicated RAN infrastructure in some critical areas, the use of dedicated spectrum whenever it is possible and the agreement of SLAs in case of hybrid models of network operation (eg, MVNO)."

Frisa continues: "Failover mechanisms between PMR, LTE and Wi-Fi are essential in order to guarantee the availability of the service for the users, and this feature has been already included in the scope of 3GPP standardisation under the paradigm of 'Interworking', understood as the continuity of services implemented across broadband and narrowband networks.

"Until this specification is completed and can be extended to other broadband technologies like Wi-Fi, some end-users are demanding proprietary solutions in order to cover their service availability requirements."

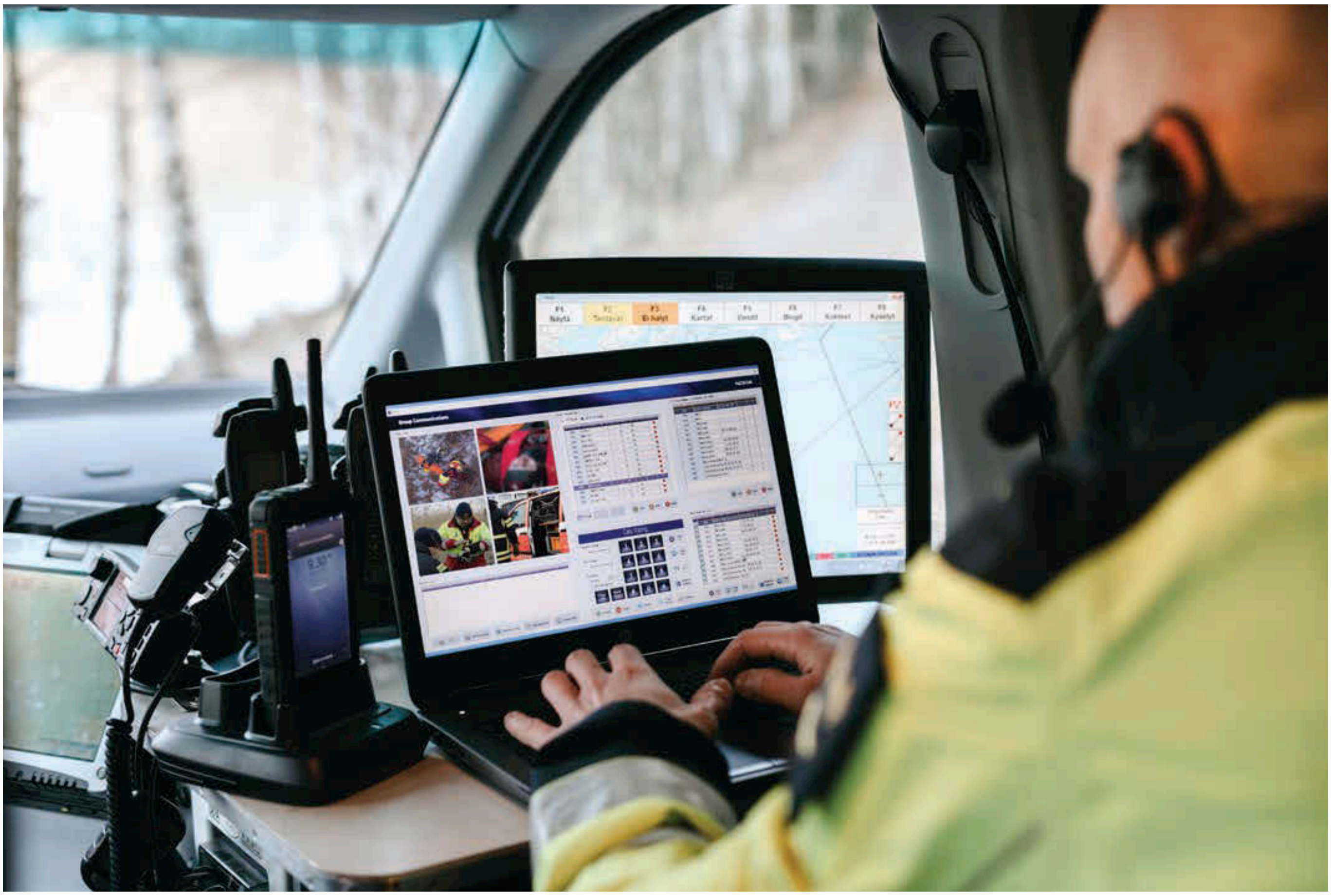
> "Failover mechanisms between PMR, LTE and Wi-Fi are essential in order to guarantee service availability"

Resilience measures for mission critical 4G LTE networks will depend to some extent on whether they are private dedicated networks with their own spectrum or commercial operators providing services to both mission critical users and consumers

The game of 9s

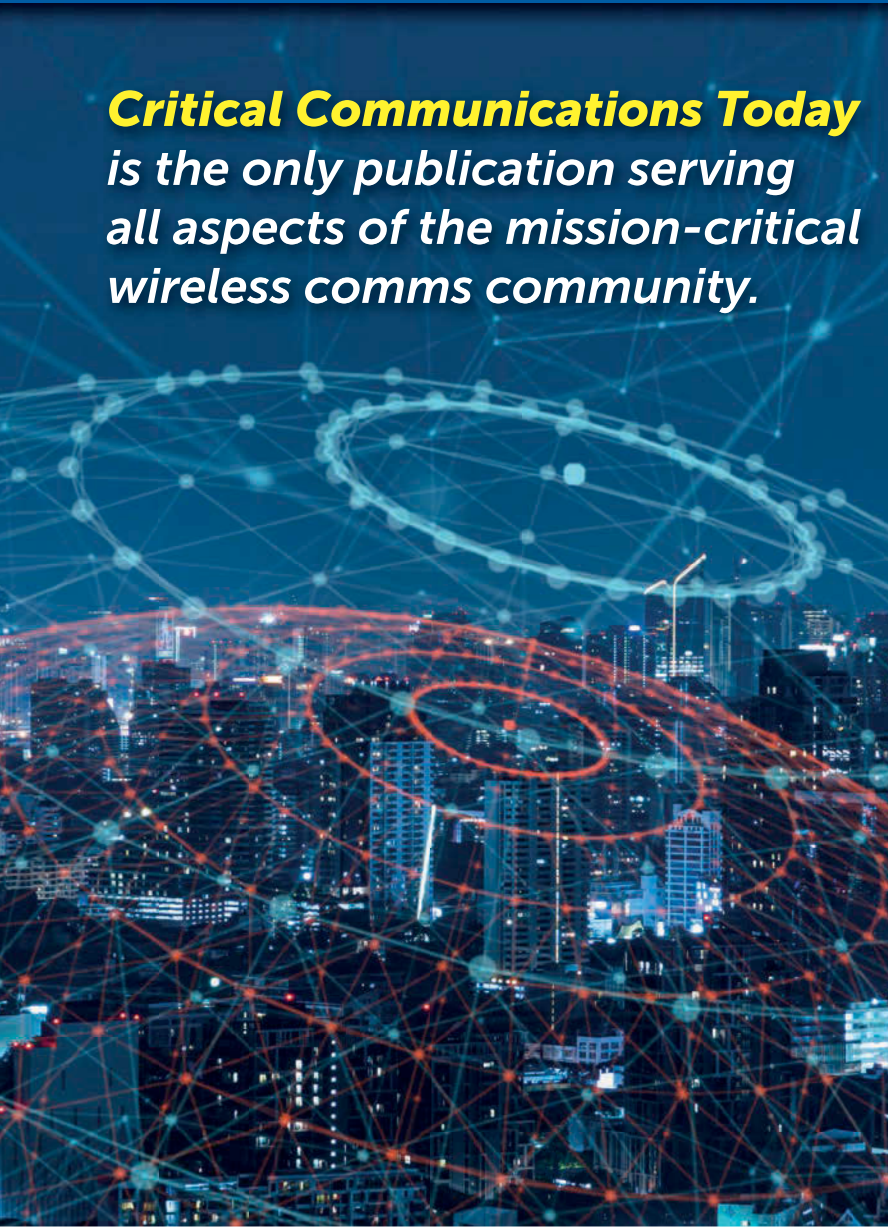
Whether the goal is 99.9 or 99.999 per cent availability, resilience will not happen without thought and planning. The approach taken by FirstNet (see box) and others in understanding the views and needs of end-users and their organisations will lay down the targets for overall resilience and areas of special need.

Careful analysis will identify the particular areas for developing resilience. Increasingly, networks are partnerships between multiple suppliers, and so establishing closely working teams with clear KPIs and service-level agreements becomes vital. Fall-back strategies which may involve using reserve equipment and personnel also need to be considered, as well as training and regular exercises.



CRITICAL
COMMUNICATIONS TODAY

The global information resource for mission-critical communications



Critical Communications Today *is the only publication serving all aspects of the mission-critical wireless comms community.*

Our reach is massive, with over

20,000

digital and printed copies

Engage with industry professionals in more than

105

different countries.

CRITICAL
COMMUNICATIONS TODAY
The global information resource for mission-critical communications
Oil & gas embraces hybrid comms
p10
Focus India
Public safety communications progress is patchy, but there are ambitious development plans for smart cities
p14
Cyber security
Migrating mission-critical users from private radio networks to public broadband brings new risks that must be managed
p20
PMRExpo 2019
Our summary of key topics discussed at the conference and some of the new products on the exhibition floor
January 2020
www.criticalcomms.com
@CritCommsToday
SUPPORTED BY
TCCA 25
PUBLIC SAFETY
TRANSPORT
INDUSTRY

Contact Andrew at
andrew.bird@markallengroup.com
if you want to take advantage of the exposure that we provide

REGISTER FOR YOUR ***FREE*** COPY TODAY

www.criticalcomms.com