

comms critical

PUBLIC SAFETY | UTILITIES | MINING | TRANSPORT | DEFENCE

PP1000007393

**A SMARTER, SAFER PATH TO
MISSION-CRITICAL BROADBAND**

Hybrid solutions that protect what
works and unlock what's next.

sepura

 **AUSTRALIA
DAMM**
Critical communication made easy

OPEN THE FUTURE

**OF MULTI-AGENCY
RESPONSE**



CRITICAL COMMS? ASK FOR OPEN STANDARDS.

taït

- 6 An introduction to interference hunting
Maintaining high quality communications
- 14 Who are the mission-critical communications
users?
- 24 Is your agency truly ready for AI in public safety?
AI is already changing what it means to run an ECC
- 29 Leveraging body worn cameras in retail
A new level of safety and security
- 33 How thousands of tiny dots could save first
responders' lives



FREE digital subscription

This bimonthly magazine is free for industry professionals in digital format.
Subscribe at: www.criticalcomms.com.au/magazine

ON THE COVER



As organisations across Australia modernise mission-critical communications, hybrid models that combine land mobile radio (LMR) with mission-critical LTE offer a practical route to MCX. They enable advanced capabilities such as video, rich data sharing and improved situational awareness, while retaining the proven reliability of technologies such as TETRA.

A successful migration should be phased, cost-conscious, and shaped around operational needs, user readiness and coverage requirements.

Incremental upgrades reduce disruption, and allow teams to test new features, gather feedback and refine processes before wider rollout. This helps manage risk while maintaining operational continuity.

Reusing existing accessories and infrastructure helps control costs and simplify deployment. Hybrid devices such as Sepura's SCU3 vehicle device and SCL3 handheld are designed to integrate with current systems and support many existing audio accessories.

Vehicle installations can also define migration timelines, particularly for large fleets. Early planning helps organisations understand costs, logistics and downtime, while solutions such as Sepura's SCU3 vehicle hub can simplify installation by combining TETRA, LTE voice, routing, Android OS and data-intensive applications in one unit.

In Australia's varied terrain, hybrid solutions provide the flexibility to switch between LTE, LMR and satellite broadband where available. TETRA device-to-device communication remains a vital fallback when 4G/5G coverage is limited.

By taking a planned, phased approach, organisations can unlock the benefits of LTE and MCX as they mature, while minimising disruption and protecting investment in proven communications technology.

www.sepura.com

Damm Australia
www.damm-aus.com.au

Do you read me?

As radio frequency communications have become ever more embedded in our daily lives, the airwaves have grown increasingly congested. Nowadays, interference hunting is no longer a niche technical skill but an essential discipline. As spectrum demand intensifies, so too does the need for skilled practitioners and robust tools capable of quickly identifying and resolving disruptive signals before they compromise critical operations.

In this issue we also turn our attention to the ongoing migration from narrowband to mission-critical broadband networks. This transition promises richer data, video and applications for frontline responders, but it also raises a fundamental question the industry has yet to fully answer: what exactly defines a 'mission-critical user'? Without a shared, agreed definition, operators, vendors and regulators risk building networks around inconsistent assumptions — potentially undermining the very reliability that broadband is meant to deliver. Establishing clarity here is not just a technical exercise, but an important step towards establishing interoperability and trust across the sector.

We also can't avoid the rise of artificial intelligence in public safety agencies — it is already here, embedded in dispatch, analytics and decision-support tools. The challenge now is ensuring it is deployed thoughtfully and with a focus on practical outcomes. It is important to avoid the common misconception that AI can be added as a bolt-on solution, and see that AI for public safety delivers the most value when it is integrated into the tools, data and workflows emergency call centres already use.

Finally, we look at body-worn cameras through a broader lens. We look at the results of a study that finds their value in deterring conflict and protecting retail staff is well established, and that they also function as one component within a wider, integrated safety and welfare toolkit — working alongside training, communications and reporting systems to create genuinely safer environments.

As always more detailed daily news and new products can be found on criticalcomms.com.au, and by subscribing to our weekly email newsletter.



Glenn Johnson, Interim Editor
cc@wfmedia.com.au



Westwick-Farrow Media
A.B.N. 22 152 305 336
www.wfmedia.com.au

Interim Editor: Glenn Johnson
cc@wfmedia.com.au

Publishing Director/MD:
Janice Williams

Art Director/Production Manager:
Linda Klobusiak

Art/Production:
Kate Atkinson

Circulation: Alex Dalland
circulation@wfmedia.com.au

Copy Control: Ashna Mehta
copy@wfmedia.com.au

Advertising Sales

Tim Thompson Ph 0421 623 958
tthompson@wfmedia.com.au

Liz Wilson Ph 0403 528 558
lwilson@wfmedia.com.au

Head Office

Unit 5, 6-8 Byfield Street, North Ryde
Locked Bag 2226,
North Ryde BC NSW 1670
Ph: +61 2 9168 2500

Print Post Approved PP100007393
ISSN No. 2202-882X
Printed and bound by IVE Group



Westwick-Farrow Media is committed to using environmentally responsible print services to produce our publications. This edition is made with a mixture of materials from FSC-certified forests, recycled materials, and/or FSC-controlled wood. While controlled wood doesn't come from FSC-certified forests, it mitigates the risk of the material originating from unacceptable sources. It is delivered in a totally degradable plastic wrapper.

All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them. Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick-Farrow Pty Ltd does not quantify the amount of local content or the accuracy of the statement made by the source.

If you have any queries regarding our privacy policy please email privacy@wfmedia.com.au

Calendar

July

ARCIA Critical Communications Conference and Qld Networking Dinner

30 July 2026

Rydges South Bank Brisbane
arcia.org.au/events/critical-communications-conference-brisbane-2026

August

RadComms 2026

25–26 August 2026

RACV City Club, Melbourne
acma.gov.au/events/2026-06/radcomms-2026

September

ACRNA Conference 2026

1–2 September 2026

The Star, Brisbane
acrna.org/conference/

ARCIA Critical Communications Conference and SA Networking Dinner

17 September 2026

National Wine Centre of Australia
arcia.org.au/events/critical-communications-conference-adelaide-2026

October

Comms Connect Melbourne 2026

14–15 October 2026

Melbourne Convention & Exhibition Centre
melbourne.comms-connect.com.au

November

PMRExpo 2026

24–26 November 2026

Koelnmesse, Germany
pmrexpo.com/en/

December

2026 IEEE Global Communications Conference

7–11 December 2026

Macau S.A.R., China
globecom2026.ieee-globecom.org/

Further event information can be found at criticalcomms.com.au/events

COVERAGE MAPS SET EXPECTATIONS

RFI EXCEEDS THEM

Engineering antennas for
Australia's toughest coverage demands



RFI
TECHNOLOGY SOLUTIONS

Scan QR Code
to find out more



The background of the page is a photograph taken from a rooftop. On the left, a large, dark, cylindrical antenna array is visible, partially obscuring the view. To the right, a black, hexagonal-shaped antenna is mounted on a metal railing. In the background, a city skyline with various buildings and a church spire is visible under a blue sky with scattered white clouds.

AN INTRODUCTION TO INTERFERENCE HUNTING

Paul Denisowski and Peter Busch, Rohde & Schwarz

The rapid rise in the prevalence and importance of radio frequency communications has increased the significance of interference hunting.



Robbie & Schwarz

INTERFERENCE HUNTING

Much of what we do today depends on having high-quality communications systems in place. Radio frequency interference, in which RF energy degrades the performance of an RF communications system, can have a significant impact on the end user's quality of experience and, in some cases, have catastrophic results. As radio systems have evolved and become more complex, and as the number of interferers has steadily increased, the importance of interference hunting has grown significantly.

For over a hundred years, radio frequency (RF) signals have been used for the transmission of information over both short and long distances. However, the last few decades have seen a fundamental shift in the nature of how these communications take place, and the risk of interference has increased dramatically.

What is interference?

The term "radio frequency interference" refers to situations in which the presence of RF energy degrades the normal operation of a wireless communications system. There are no specific level or frequency criteria that must be met in order for something to be considered interference: signals that affect the service of an application may have no negative effect on other applications. Simply put, the definition of interference is a purely functional one: any radio frequency signal that has a negative impact on the ability to operate a wireless communications system can be considered interference.

Effects of interference

The effects can vary tremendously depending on the characteristics of both the interferer and the affected system. In fact, the very first step in interference hunting is to detect the presence of interference. In some cases, poor system performance may be due to design issues rather than interference.

Fortunately, there are certain common symptoms that can indicate the presence of interference. For example, in analog voice communications systems, interference often becomes immediately apparent to users in the form of noise, static, superimposed audio and unexplained breaks in squelch.

In digitally modulated communications systems, the presence of interference is often not immediately obvious. Poor voice quality is one indication of possible interference, although voice quality can depend on a variety of factors. A more reliable indicator of interference in digital networks is dropped calls or lost connections. Low data throughput or high retransmission rates are also good indications >>



ANALYSING SUSPECTED INTERFERERS IS IMPORTANT FOR A NUMBER OF REASONS, NOT THE LEAST OF WHICH IS CONFIRMING THAT A RECEIVED SIGNAL IS ACTUALLY INTERFERENCE.

that some form of interference may be present. Owing to the adaptive nature of many modern communications systems, interference in digital networks can cause the system to revert to more robust transmission modes or lower-order modulation types; communications may still be possible, but with substantially degraded performance. Furthermore, the severity of these effects may not increase linearly with the level of interference.

What is interference hunting?

In some cases, it is possible to compensate for interference without actually shutting down the interferer. For example, the use of shielding or filters, changing antenna orientation, changing frequencies, etc, can limit the effects of the interfering signal on the affected device. However, in the vast majority of cases the only way to eliminate the interfering signal is to identify, locate and disable it. The process by which an interfering signal is identified and located is called interference hunting.

As mentioned above, the first step in interference hunting is recognising that there is interference. A related and equally important task is analysis of the behaviour, spectral characteristics and (if possible) content of the interfering signal. There are some interfering signals that can be identified and located by analysis alone. For example, if interference is being caused by an analog audio transmission, listening to the content of the transmission may yield information that indicates its source. Even if such precise identification is not possible, analysing the spectrum and behaviour of an interferer can provide valuable clues for further investigation.

But even when analysis of the interferer gives us a strong indication as to its origins, it is almost always necessary to identify the precise location of the device generating the interference. This is the second and most challenging component in interference hunting, namely radiolocation or direction finding.

Steps in interference hunting

Before beginning interference hunting, it is important to be reasonably sure that external interference is present and to have some idea as to the spectral characteristics of the interfering signal.

If interference is suspected, the next step is to identify the general geographical area in

which the interference occurs. The diameter of this area will vary depending on factors such as the type of service, terrain and propagation, but tends to be in the order of several kilometres.

Field work can be started once this general geographic area has been identified. Vehicle-mounted automatic direction-finding or drive test systems can be used in this phase, although handheld antennas and portable instruments are also effective tools. If the interfering signal is visible over larger distances, bearings and triangulation may be used to estimate the interferer's position. The goal in this stage is to restrict the search location to a walkable area such as a city block and group of buildings.

The final step in interference hunting involves walking around the suspected interferer location and taking measurements using a handheld instrument and directional antenna. Here, the usual methodology is to scan or sweep buildings or structures, concentrating on devices that are known radio frequency emitters, such as antennas and electronic devices. Unlike the first two steps, this step often requires physical access to private property or premises.

Interference hunting tools

The two most common instruments that are used in interference hunting are spectrum analysers and monitoring receivers.

Spectrum analysers use a heterodyne or swept architecture. The input signal in question is converted to an intermediate frequency using a mixer, and a local oscillator provides the mix frequency. The intermediate signal is then swept past a fixed-tuned filter (the resolution bandwidth), logarithmically amplified and sent to the display.

Monitoring receivers, on the other hand, digitise the input signal and then apply a fast Fourier transform (FFT) to generate the displayed spectrum. As a result, monitoring receivers are substantially faster and more sensitive than swept spectrum analysers.

Since almost all interference hunting involves a walking/sweeping stage, it is important that instruments used in interference hunting are battery-powered, portable and reasonably rugged.

The other indispensable tools in interference hunting are antennas. In order to effectively detect an interfering signal, we

need either an antenna that is matched to the frequency of interest or a wideband antenna that is capable of efficiently receiving signals at a wide range of frequencies. Although omnidirectional antennas are often used in the driving-around stage of interference hunting, locating interference sources requires the use of a directional antenna. In most cases, directional antennas are handheld Yagi, log-periodic or dipole antennas. The direction of the interference source can be determined by pointing the antenna in different directions and monitoring the signal.

There are also special direction-finding antennas that, when connected to a direction-finding receiver, can be used to automatically calculate the direction or bearing of a signal source. These systems may be based on a variety of direction-finding methods (Doppler, Watson-Watt, TDOA, correlative interferometer, etc) and are either always mounted on a vehicle or set up in a fixed location. In many cases, these systems are able to automatically determine an interferer's location within a radius of several dozen metres.

Perhaps the most important tool in interference hunting is knowledge of radio frequency principles, propagation, signals and spectral allocations. Having the right tools, a familiarity with the signals normally found in a given region of spectrum, and knowledge of the characteristics of common interferers is essential for quick and efficient identification and resolution of interference issues.

Analysing interference

Analysing suspected interferers is important for a number of reasons, not the least of which is confirming that a received signal is actually interference. Detailed analysis of an interfering signal can also provide vital clues about its source and even its location. For example, if our interfering signal consists of a regular, contiguous pattern of 8 MHz-wide haystacks of almost identical amplitude, it is extremely likely that this signal is egress from a cable television system, and our efforts can be focused on examining cable-related infrastructure and devices (8 MHz is the typical bandwidth for a TV channel).

There are several different ways of analysing interference, and interference hunting often requires a combination of these analysis methods. The most basic method for analysing interference is visual inspection of the spectrum. The traditional method for displaying spectrum is a graph of amplitude versus frequency. In a waterfall or spectrogram display, the vertical axis represents time and different colours are used to show amplitude. This type of



iStock.com/bjdlzx

display is extremely useful for analysing intermittent or variable frequency signals. For most interference-hunting applications, the simultaneous display of both spectrum and waterfall provides the user with an optimal mix of information. Additional numerical data can be obtained using markers and lines.

Another useful interference analysis method is behaviour or pattern analysis. Interference sources may be continuous in nature, ie, always on, while others may be intermittent over shorter or longer periods of time. Knowing that a given type of interference only occurs during home football games at night is a powerful indicator of where that interference might be coming from. Similarly, problems that only occur when it rains or is very windy suggest outdoor sources. Possible correlation between interference and other events should always be considered, no matter how unrelated the events may seem.

Further useful capabilities for analysing intermittent interference include remotely accessing and controlling an instrument, triggering and collecting information when interesting events occur, and recording spectral data over a long period of time for later analysis. Spending hours staring at a screen and hoping to catch an intermittent interferer is not an effective or popular interference-hunting method.

Common interference types

While the variety of interference sources is almost endless, a large number of (especially narrowband) interferers often share common

characteristics. An awareness of these frequently reoccurring themes can save a significant amount of time and effort when investigating potential interference sources.

It is useful to differentiate between noise created by electrical systems and noise created by electronic systems. Electrical noise sources tend to be many megahertz wide and may be periodic in frequency or time. Examples of this are emissions from electric motors, welding equipment, vehicle ignition systems, electric fences and faulty transformers/ballasts. In contrast, noise from electronic sources, sometimes also referred to as spurious emissions or spurs, are usually much narrower (less than 1 MHz wide) and tend to be continuous, although in some cases they may vary in frequency, ie, be oscillating or drifting. It is fairly safe to say that almost all consumer and commercial electronics radiate spurious emissions at numerous frequencies; it is the level of these emissions that determines whether or not they are sources of interference.

A jammer preventing communications

There are sometimes cases of deliberate interference, in which someone intentionally interferes with radio frequency communications. Unfortunately, there are many cases of individuals making unauthorised, harassing or misleading transmissions on public safety, government, commercial and amateur radio frequencies.

The other most common source of deliberate interference is jammers: devices designed to limit or deny the ability to use a certain

frequency range by raising the noise floor to an extremely high level — typically around -50 dBm in the affected area. Jammers are often designed to affect particular services (GPS, Wi-Fi, etc) or frequency bands (850 MHz, 1900 MHz, etc), but often create issues for services and frequencies well outside of their target range. In order to be effective, a jammer must generate a wide, strong, continuous signal, and this makes it relatively easy to identify and locate them. Most jammers have multiple antennas (one per target service/band), but may also be disguised as everyday objects.

It is important to keep in mind that although most individuals and organisations are very cooperative in helping to resolve interference issues, persons who deliberately cause interference will often go to great lengths to disguise and deny their activities.

Summary

The rapid rise in both the prevalence and the importance of radio frequency communications has increased the significance of interference hunting as a means to identify and resolve interference issues as quickly and efficiently as possible. While there is tremendous variation in the types and sources of radio frequency interference, knowledge of common causes and characteristics, together with the use of appropriate tools and techniques, greatly increases the probability of locating and resolving these issues.

This article is based on a Rohde & Schwarz white paper at <https://bit.ly/3SX8SKY>

COMTECH TO SELL ITS SPACE AND SATELLITE BUSINESS

Comtech Telecommunications has announced that it has entered into an agreement to sell most of its satellite and space communications business to Gilat Satellite Networks and become a focused public safety technology company.

Under the terms of the agreement, Gilat will acquire most of the satellite and space business for US\$157.5 million. Comtech will retain certain cyber-focused assets currently within the satellite and space business.

"The sale of most of the S&S segment, together with the agreements we have reached with our lenders and preferred stockholders, represent a significant milestone in Comtech's transformation and reflect the successful execution of our strategy," said Ken Traub, Chairman, President and CEO.

Upon closing the transaction, the company will align its operations, strategy and brand with its public safety focus and will transition to the Allerium name.

"Over the next few months as we await regulatory approval, we will be executing a transition plan to align the organisation to be purpose-built to support Allerium's growth as a leader in next-generation public safety technologies and services," Traub said.

The company says Allerium will be able to direct investment, innovation and execution around a single mission-critical market with significant long-term demand drivers as public safety solutions continue



istock.com/NicoFino

to evolve from voice-based connections to data-centric communication, coordination and real-time AI-enhanced decision-making.

"Allerium is well-positioned to build upon the leadership we have established in the public safety market, as we are the first to bring together the complete emergency response ecosystem — from device location to the systems, networks and data analysis that help drive action and connect people to emergency assistance," said Jeff Robertson, President of Allerium.

"We are impressed with the successful progress of Comtech and look forward to welcoming its Satellite and Space Communications segment into Gilat," said Adi Sfadia, CEO of Gilat. "This segment brings a talented team and strong technology, and we believe it is an excellent strategic fit with Gilat."

MOTOROLA SOLUTIONS EXPANDING ASSIST AI GLOBALLY



istock.com/Jacob Wackerhausen

Motorola Solutions has announced the global expansion of Assist, its mission-critical AI for public safety. Following successful deployments across US public safety agencies, the capability is scaling internationally to bring role-specific intelligence to control room operators, emergency responders and investigators.

"Emergency personnel face an overwhelming influx of data under immense stress," said Fergus Mayne, vice president of

sales, Europe, at Motorola Solutions. "By automating routine tasks and surfacing vital insights in real time, Assist cuts through the noise. It reduces the immense cognitive load on frontline teams, empowering them to respond to critical incidents with greater clarity, speed and confidence."

Motorola says Assist layers intelligent capabilities directly into Motorola Solutions' control room software to help accelerate emergency response. It automatically identifies, gathers and prioritises vital call information — such as historical incident data at a specific location or critical keywords like 'heart attack'. To minimise miscommunication and preserve operator focus, Assist supports live transcription, call language translation, advanced audio enhancement and a non-emergency call agent that automatically handles routine calls to allow human operators to focus on critical emergencies.

For staff in the field, Assist is a mobile-first digital force multiplier at the edge to help enhance productivity, situational awareness and safety, while for investigators handling large volumes of evidence, Redaction Assist leverages automated object and speaker tracking within the evidence management workflow. It can automatically tag evidence and redact sensitive subjects and objects to accelerate records documentation and support privacy.

**Mining version IS380.M1 –
coming soon!**

4G Radio **IS380.1**

Familiar feel. Unlimited reach.
This new 4G radio makes the switch effortless.

Built for hazardous environments and certified for Zone 1/21, the IS380.1 runs on ISM-OS 16 and delivers Push-to-Talk over Cellular and Mission Critical PTT over existing 4G networks. It looks and handles like the radio your teams already know – but now your voice travels far beyond the site boundary. No new workflows. No retraining. Just wider, smarter communication.

- › **Android-based 4G radio** – combines telephony and push-to-talk (PTT) in one handy device
- › **Familiar two-way radio design** – enables easy transition from classic radios to the IS380.1
- › **Supports MCPTx communication** – compliant with the 3GPP standard
- › **Replaceable battery** – enables continuous operation readiness
- › **Rotary switch for channel selection or volume control** – enables quick and safe handling
- › **System integrated i.safe MOBILE App World** – enables the use of certain applications for PTT & LWP



i.safe MOBILE

isafe-mobile.com

NEW ZEALAND LAUNCHES NEW CRITICAL COMMUNICATIONS ENTITY

New Zealand's SafetyNet Critical Communications (SafetyNet) launched on 1 July and is already delivering on its mandate to modernise the communications capability of New Zealand's emergency services and wider public safety sector.

Previously called Next Generation Critical Communications, last November government approved the entity's exit from its host, NZ Police. As an independent Crown company, SafetyNet can now offer its emergency-grade communications services in a commercial model to the hundreds of organisations across New Zealand's public safety sector, including central and local government agencies, Iwi, not-for-profit organisations, and infrastructure and utilities companies.

Steve Ferguson, SafetyNet's CEO, said the new organisation's priority remains delivering the Public Safety Network's (PSN) 500-site digital Land Mobile Radio network for foundation customers Police, Fire and Emergency New Zealand, Wellington Free Ambulance and Hato Hone St John.

SafetyNet has also begun a carefully managed process of onboarding the first new PSN cellular services customers including the National Emergency Management Agency, Surf Lifesaving New Zealand, Selwyn District Council and Maritime New Zealand.

Michael Clulow, Manager Operations for Maritime NZ's Rescue Coordination Centre New Zealand, said having PSN Cellular Services will boost the communications capability underpinning its vital search and rescue operations.



istock.com/nazir_ah

"Adding Public Safety Network Cellular Services to our communications infrastructure ensures additional resilience to our systems, enabling us to deliver our 24/7 safety of life service during a significant national event or during periods of network outages. By joining SafetyNet we have added confidence that we can help those in need, whenever and wherever they need it," he said.

"Since 2022, using a collaborative model, we have delivered the emergency services with three globally leading cellular services, and a new voice console. Our experts have also delivered the Device Location Service which helps the emergency services to locate the phones of people who are at high risk," Ferguson said. "Delivery of the 500-site new Land Mobile Radio network is underway with the first region aiming for go-live in Canterbury late this year."

MYRIOTA LAUNCHES HYBRID 5G SATELLITE AND CELLULAR IOT NETWORK



Satellite IoT company Myriota has announced the addition of cellular connectivity to its HyperPulse 5G non-terrestrial network (NTN) and AssetHawk asset tracker device, creating a hybrid IoT network that enables seamless asset tracking between cellular coverage and remote, zero-cell environments.

By combining HyperPulse's low-power satellite connectivity with support for cellular networks, Myriota says it is delivering a hybrid solution designed for industrial IoT at scale. HyperPulse automatically routes each message across cellular or satellite based on availability and configuration, removing the need for users to manage separate satellite and cellular providers, contracts

and platforms. A single device on a single connectivity contract now covers the full operational geography of an asset, from urban logistics hubs to the most remote environments on Earth.

The addition of cellular lowers the blended cost per message by seamlessly routing to the most cost-effective network, with hybrid data plans starting at US\$0.99 per device per month.

"The launch of hybrid connectivity for HyperPulse and AssetHawk further cements Myriota's position as a global provider of scalable IoT connectivity, enabling organisations to keep assets continuously connected across both terrestrial and non-terrestrial networks, and turn real-world operational data into action," said Ben Cade, CEO of Myriota. "For decades, vast numbers of remote and distributed operational assets have remained disconnected — not because the technology didn't exist, but because the economics never worked."

Satellite IoT has historically served the most remote use cases. Adding cellular changes the economics for a far broader asset class: vehicles moving along transport corridors, generators rotating between sites, or containers transitioning through ports before moving inland. These assets spend only part of their working life outside terrestrial coverage — enough to need satellite coverage, but not enough to justify satellite-only economics.

"For the first time, it's commercially viable to connect almost any asset, anywhere, for less than a dollar per month, making this one of the most accessible solutions available today," Cade said. "That's not an incremental improvement — it's a whole new market."

R&S® PR200 portable monitoring receiver

THE FIELD EXPERT



The R&S®PR200 portable monitoring receiver is an indispensable tool for interference hunting and various other radiomonitoring tasks. Due to its excellent RF performance in its class, it can even handle complex spectrum environments. The compact and light-weight receiver offers high signal processing speed, field-tested usability and delivers a bandwidth of up to 40 MHz in real time. Several options and accessories allow individual configurations and also make it a field expert for future applications.

For more info: www.rohde-schwarz.com/product/PR200

ROHDE & SCHWARZ

Make ideas real





WHO ARE THE MISSION-CRITICAL COMMUNICATIONS USERS?

TCCA Limited

In the transition from narrowband to mission-critical broadband networks there will need to be an agreed definition of a 'mission-critical user'.

There are many types of operations that rely on critical communications. These include public safety and security, emergency services, critical infrastructure, public utilities, transportation, critical industries and related activities, where failures in critical communications would lead to catastrophic degradation of services. Yet there is no clear definition of a 'mission-critical user'.

To date it has been each country itself that defines the users of their mission critical network. This is reflected in the findings from a survey carried out by TCCA's Legal and Regulatory Working Group (LRWG). The survey gathered information on users that have access to the mission-critical network (MCN) in the United Kingdom, Denmark, Hungary, Netherlands, Spain, Norway, Finland and Germany. In the survey, the governmental agencies operating the MCN were asked to provide information regarding the definition of users, both for the existing narrowband networks and the new broadband networks.

The findings form the basis for the new white paper *Definition of Users in Mission Critical Networks*. The paper highlights that there is no clear common approach or definition of user groups that are given access to the mission-critical network. Apart from the first responders — police, fire and rescue, and ambulance services — the user groups vary from country to country, and sometimes even from region to region and network to network.

The transition from narrowband to broadband services

Today, a majority of countries that operate mission-critical networks rely on state-owned dedicated narrowband systems such as TETRA networks, open only to critical users. However, as critical communications transition to broadband services, they will be utilising commercial networks shared with commercial users. This puts a reliance on commercial mobile network operators to provide mission-critical user requirements.

A majority of the countries that provide mission-critical networks (MCNs) are currently working on a transition to mission-critical broadband networks (MCBNs). As the new MCBNs will be based on the commercial networks, the transition must entail a transfer of the high security and reliability features that emergency services across the globe have come to rely on from the current legacy networks.

In addition to this, the users of the MCN also have special requirements compared to ordinary commercial users that will need to be enabled in the commercial networks regarding Quality of Service, Priority and Pre-emption (QPP), hence the need for a common definition of a 'mission-critical user'.

Since not all users of the commercial networks can benefit from the features and advantages of MCBN, there will be a need to define who the users of the MCBN shall be.

A definition may also be required in cases where a country wishes to establish an internal hierarchy within the MCBN in order to dedicate QPP to certain resources in the event of capacity limitations.

Cross-border cooperation

In many parts of the world, such as in Europe, there are also plans to interconnect mission-critical broadband networks across national borders in order to enable and support seamless cooperation and collaboration between countries, such as the planned European Critical Communications System (EUCCS). Additionally, Great Britain and France will have to enable interworking between the Emergency Services Network (ESN) and Réseau Radio du Futur (RRF), to aid cooperation in and around the Channel Tunnel.

In the case of bilateral relations, a common understanding in operational aspects is critically important, for example, when roaming across networks. This raises the question of which users are to be accepted and can gain access to the visited network. If the definition of 'user' differs significantly between networks and agencies, enabling roaming would be operationally complicated.

Agreed terminology

Over the years, the wider telecommunication sector has developed a set of terms with globally accepted definitions, and this has contributed to the overall development of the sector. Norms in terminology help improve collaboration, leading to innovation and economies of scale. The critical communication sector should also follow this path to foster strong collaboration between all stakeholders.

"The critical communication sector is comparatively much smaller than the consumer sector, so critical communication agencies have come to realise that they have to work closely together," said Nina Myren, LRWG chair and TCCA Board member. "Close collaboration requires a common

>>



approaches to the MCN utilisation; mandatory, voluntary or approval-based MCN usage. The survey results show that half of the countries have legally obliged users to use the existing MCN through national laws. The obligations primarily cover Blue Light organisations, and to some extent the military. In all the surveyed countries, other users must be formally approved in order to become users of the MCN.

User priority levels

The survey also examined whether user groups have different priority levels within the MCN. Many responding countries replied that no such measures are applied, meaning that all users are treated equally. However just under half confirmed that priority levels are implemented, granting certain user groups higher priority during network congestion. The type of priority levels applied vary by country and consist of mechanisms such as organisational level prioritisation, prioritisation based on operational needs and prioritisation of specific talk groups such as emergency talk groups.

Responses from the survey indicate countries plan to continue with the same practice as applied today and at least one country intends to implement the user hierarchy in the MCBN in a different manner than in the existing MCN, indicating a further need to reassess user definition in light of the added functionality and complexity associated with MCBN.

Recommendations

The LRWG is of the view that it is beneficial for the critical communication sector to consider setting a definition of the user through legislation. An option is to establish a common definition or setting minimum criteria defining core users, mainly in the form of the Blue Light organisations, which would largely correspond to an 'emergency service' as defined in existing legislation. Additionally, legislation could define other users who may utilise the MCBN and MCN in accordance with national practice and thereby require mutual recognition of such users amongst interconnected countries.

In addition to the definition of users, it may be relevant to define mission critical functionalities that the MCBN should generally support. This is to ensure that users visiting another country can have access to the same or similar levels of functionalities as in their home networks thereby optimising operational mobility.

“ IN ADDITION TO THE DEFINITION OF USERS, IT MAY BE RELEVANT TO DEFINE MISSION CRITICAL FUNCTIONALITIES THAT THE MCBN SHOULD GENERALLY SUPPORT.

understanding and common approaches, and for common approaches to be effective, the terminology used must have the same or similar meaning throughout the sector and across the agencies.”

The term 'user' is thus a key term that requires a common definition, not least as a prerequisite for effective cross-border communication.

As a result of the global trend of moving towards MCBN with enhanced technical functionalities, cross-border interoperability and cooperation between critical communication agencies is expected to improve significantly. An example of this is the EUCCS that aims to connect national MCBNs through seamless critical communication and operational mobility across the EU and Schengen area in order to strengthen public safety and civil protection.

Blue Light organisations users and 'other' users

The Blue Light organisations (police, fire, rescue and ambulance) form the core users of the MCN in all the countries surveyed by the LRWG. In addition, several countries have enabled other user groups to use the MCN.

The category of other users that have access to the MCN in the countries span a broad range of sectors and entities, reflecting distinct national approaches to safety and civil contingency. Examples include users within the military and customs authorities as well as critical infrastructure operators such as utility companies. Some countries also include non-state organisations that support emergency services, such as the Red Cross and Mountain Rescue in Norway.

The LRWG identified three main

Spectrum Analysers, Electronic Counter-surveillance Systems, Software-Defined Radio and general Test & Measurement



Signal Generators

- Tracking generators to 12.4GHz
- Vector Signal Generators for arbitrary waveform generation to 20GHz



The PCR4200, 4-channel, phase coherent receiver

- 100kHz - 20GHz
- Simultaneous multi-band spectrum monitoring
- Emitter detection and geolocation
- Multi-channel transmitter testing
- SIGINT/COMINT/ELINT
- Drone detection
- MIMO channel testing

Aaronia antennas and accessories



Spectrum Analysers

- Models for 1Hz – 43GHz
- USB and SFP+ models
- TeraHertz sampling speeds!



EXCLUSIVE
DISTRIBUTOR FOR
AUSTRALIA AND
NEW ZEALAND.

- FULL FUNCTION SPECTRUM ANALYSER ON YOUR PC OR LAPTOP
- WINDOWS AND LINUX SOFTWARE SUPPLIED
- FULL API SUPPORT FOR CUSTOM APPLICATIONS
- 5G/LTE TESTING
- SPECTRUM MONITORING
- INTERFERENCE TESTING
- WORKSHOP, LAB AND HOBBYIST APPLICATIONS
- GOVERNMENT AND DEFENCE USERS



Silvertone

UAV & Communications Specialists

1/21 Nagle Street Wagga Wagga NSW 2650

Phone (02) 6931 8252

contact@silvertone.com.au

silvertoneelectronics.com

FULL SPECIFICATIONS ON OUR WEBSITE.

Industry Talking



The ARCIA mid-year update starts with a thank you to all our members and partners. The last financial year has seen growth in terms of memberships, partners and engagement, and it has been fantastic to see our industry community come together around the country. Whether it be for training, conferences, sundowners or dinners, the community is thirsty for information and to get together as often as possible.

The Sydney conference was well attended and the topics discussed were current, with newer technologies like satellite making a big impact in a short period of time. There are, as there always have been, challenges getting end users to these events, despite the best efforts of our team, given everyone is so busy, but I do encourage you to get along when you can, as the benefits are varied and valuable. The NSW state networking dinner was very enjoyable, and where we recognised Peter Maggill, from Parkes NSW, for his very long-term commitment and operation as a regional radio dealer, with the NSW State Professional of the Year award. Congratulations to Peter, a very worthy winner of the 2026 award.

As you may have seen, the committee has made the decision, based on market feedback, to add a Victoria dinner this year, having been asked over the last couple of years to have a dinner similar in format to the other states. It will also give the association a platform to present the State Professional of the Year Award in Victoria, with worthy recognition of such an honour for the recipient. So, add 5 August to your events calendar, as we hope to see as many locals there as possible, taking advantage of this additional networking opportunity.

The next major event will be Brisbane on 30 July, with our Queensland Conference and State Dinner, where I'm sure the ARCIA team will once again organise a terrific program for both the day and night events. I am told we will have a special guest for the conference discussing the 2032 Olympics and how local business can become as engaged as possible. Bookings are open, so head to the ARCIA website and secure your team's places in the coming days, if you haven't already, as time is running out.



Hamish Duff
President (Hon),
ARCIA – Australia's Radio & Critical
Communications Association



PON analyser

As broadband and telecommunications networks continue to evolve, field technicians and service providers require test equipment that delivers precision, reliability and operational efficiency. The VeEX PX92 PON analyser and multi-gigabit service test set is engineered to meet these demands with a professional-grade solution designed for today's high-performance network environments.

Purpose-built for technicians, contractors and network operators, the PX92 provides testing capabilities across broadband and telecommunications infrastructures, helping teams streamline construction, installation, service activation and maintenance, and troubleshooting workflows with greater confidence and accuracy. By integrating PON analysis, multi-gigabit Ethernet testing, Wi-Fi performance validation and ONT emulation into a single handheld platform, technicians can verify optical signal levels, validate network throughput, and confirm Wi-Fi performance in the field, all while generating a digital compliance certificate.

For the Australian market, the VeEX PX92 has been tested and approved by NBN Co, providing assurance for technicians and contractors working within NBN environments, and confirming the PX92 as a trusted solution aligned with the practical requirements of modern network deployment and service assurance applications.

The PX92 is designed to help technicians reduce repeat site visits, improve first-time resolution rates, and maintain high standards of service delivery. Its professional field-ready design and advanced testing capability make it a suitable asset for organisations focused on network quality and operational efficiency.

TelecomTest Solutions

www.telecomtest.com.au

RFS command trailer has 24-hr power reserve



NSW Rural Fire Service (NSW RFS) is the world's largest volunteer fire service, responsible for providing fire and emergency services to approximately 95% of New South Wales. Operating across vast and often remote regions, NSW RFS plays a critical role in responding to bushfires, floods and other natural disasters.

To strengthen its frontline response capability, NSW RFS developed a Mobile Command Trailer designed to be rapidly deployed into disaster zones, providing operational coordination where it is needed most.

Natural disasters such as bushfires and floods often impact remote or infrastructure-compromised areas where access to reliable power is limited or unavailable.

NSW RFS required a fully self-sufficient Mobile Command Trailer with reliable power capable of sustaining operations for up to 24 hours in the field. The solution needed to support sensitive communications and coordination equipment, and needed to have the flexibility to be deployed directly into active disaster zones instead of relying solely on fixed regional offices.

Ensuring continuous, dependable power in unpredictable and harsh Australian environments was the primary technical challenge.

RFI partnered with NSW RFS to deliver a robust, field-ready energy system for the Mobile Command Trailer. To meet the rigorous operational demands, RFI designed and engineered an advanced 48 VDC battery storage and power management system built exclusively around PowerPlus Energy lithium storage and a high-performance Victron Energy ecosystem.

The system utilises a scaled parallel layout featuring 16 PowerPlus Energy LiFe4838P self-managed batteries, delivering a combined, resilient storage capacity of 60.8 kWh. Power conversion is managed through three Victron Quattro 8 kVA inverter/chargers providing 3-phase power, in order to ensure maximum system redundancy and seamless power delivery to mission-critical communications gear. Supplementary power is also provided from 3.7 kW of Suntech 415W

solar modules on the roof, helping keep communications connected in all conditions. System performance and real-time telemetry are funnelled through a high-resolution touchscreen interface, allowing field operators complete on-ground visibility.

The project was completed over an 18-month period and involved close collaboration between RFI, PowerPlus Energy and NSW RFS engineering teams, with installation performed by Active Electrical Australia Pty Ltd, contributing to the successful rollout.

With the Mobile Command Trailer now operational, NSW RFS has significantly enhanced its disaster response capability.

Command infrastructure can now be positioned directly in disaster zones, providing operational independence and reduced reliance on regional offices. This in turn improves community response, with faster coordination during bushfires and floods, and enhanced resilience, with reliable 24-hour power capability in remote environments.

This solution enables NSW RFS to respond more efficiently during critical disaster recovery efforts, providing faster on-ground assistance and improving operational continuity when communities need it most.

"The Mobile Command Trailer significantly enhances our ability to respond rapidly to disasters across New South Wales," said Brendan Doyle, Manager Logistics NSW Rural Fire Service. "Having a self-sufficient power solution that can reliably operate for extended periods in the field means we can establish command operations exactly where they're needed — without relying on fixed infrastructure. This capability strengthens our frontline response and ultimately helps us support communities faster during critical incidents."

Following the successful rollout, NSW RFS continues to partner with RFI for technical support, firmware optimisation and future fleet collaboration.

RFI Technology Solutions
www.rfi.com.au



Communication service monitor

Viavi Solutions has announced a TETRA MS radio base station simulator option for its field-portable CX300 communications service monitor. The upgrade enables full testing without placing radios in T1 test mode, streamlining and accelerating validation of mission-critical communication systems.

The TETRA MS upgrade is available via a software-keyed option on the CX300 and requires no additional hardware. It enables the full testing of TETRA MS radios, including transmitter parametric measurements (power profile, RF power, carrier frequency offset, burst timing, modulation accuracy), call processing and receiver BER/MER loopback without requiring the radio under test to be placed in T1 test mode. VIAVI also provides migration support for existing users of its legacy 3920B platform.

The CX300 supports the testing of all major LMR/PMR protocols including TETRA, P25, DMR (MOTOTRBO) and NXDN. The device integrates spectrum analysis, signal generation and analysis, cable and antenna analysis, 2-port 1 path VNA, power measurement, audio analysis and VIAVI AutoTest automated alignment.

VIAVI Solutions Inc

www.viavisolutions.com.au



Dual-band GNSS timing antenna

The AU-500 from Furuno is a high-performance, dual-band (L1/L5) multi-constellation GNSS timing antenna engineered to provide robust time synchronisation for mission-critical infrastructure, including 5G base stations, timing systems and communications networks. Built for performance in harsh weather and hostile RF environments, the AU-500 is designed to enable reliable operation where service outages are not permitted.

A defining feature of the AU-500 is the integrated lightning protection, compliant with IEC 61000-4-5 standards. By incorporating this protection directly into the antenna assembly, the unit provides for the safety and longevity of both the antenna and connected receiver equipment.

The AU-500 features advanced interference rejection, with a built-in noise filter that effectively removes out-of-band radio waves from LTE, broadcasting that can adversely affect GNSS reception. The underside of the main unit is also designed to function as an integrated ground plane, which improves reception sensitivity and front-to-back ratio while simultaneously reducing multipath effects. The antenna is rated to IP67, featuring a high-quality polymer radome that provides long-term protection against rain, snow, ultraviolet rays, chemicals and corrosive gases. The AU-500 is manufactured in Japan meeting the highest quality standards, including CE, FCC and RoHS 2 compliance.

Step Global Pty Ltd

www.stepglobal.com

Software-based RoIP gateways

Omnitronics has announced the launch of its next-generation omniGateDMR and omniGateP25 radio-over-IP (RoIP) gateways. These gateways are now 100% software-based, with vocoder functionality fully integrated into the software stack, eliminating the need for dedicated hardware.

The release complements Omnitronics' existing fully software DAMM TETRA gateway. The omniGateDMR and omniGateP25 gateways are designed to meet the evolving demands of public safety, utility, transportation and resource sectors, where flexibility, uptime and cost-efficiency are critical.

Benefits of the omniGateDMR and omniGateP25 software gateways include instant scalability, being able to add up to 256 talkpaths and 128 console connections in minutes with no hardware or site visits. Built-in redundancy helps ensure 24/7 uptime with high availability, automatic failover and disaster recovery managed virtually.

Users can bridge P25, DMR, analog and SIP protocols in one unified platform, and centralised remote management eliminates costly site travel by managing remote radio sites from a central control room. Being software-based, the technology can stay current with evolving standards like P25 Phase 2 and DMR Tier III through software updates.

The omniGateDMR and omniGateP25 RoIP gateways are fully compatible with the Omnitronics suite of omnicore Dispatch solutions, as well as third party dispatch systems, offering a complete end-to-end software-based radio dispatch and interoperability platform.

Omnitronics Pty Ltd

www.omnitronicsworld.com

FIXED WIRELESS FOR HEAVY INDUSTRY



WHEN OPERATIONS CAN'T STOP. NEITHER CAN THE LINK.

Connect teams, systems and remote assets with
Cambium Networks PMP 450v fixed wireless.

MINING

RAIL

PORTS



PMP 450v AP

FIXED WIRELESS ACCESS POINT



PMP 450v SM

SUBSCRIBER MODULE + PTP BACKHAUL

5.15–7.125 GHz

MULTI-BAND OPERATION

INDUSTRIAL RADIO

BUILT TOUGH FOR DEMANDING SITES

IP66 / IP67

PMP 450v SM INGRESS RATING

–40°C TO +60°C OPERATING RANGE • 200 km/h WIND SURVIVAL • AES ENCRYPTION

AP ingress rating: IP55 • SM ingress ratings: IP66/IP67



BUILD A STRONGER INDUSTRIAL NETWORK.

Talk to Streakwave about PMP 450v access, backhaul and deployment design.

sales@streakwave.com.au • +61 3 9001 4295

streakwave.com.au • Ground Floor, 470 St Kilda Road, Melbourne VIC 3004



SCAN TO CONTACT US

Frequency availability and performance vary by regulatory domain, configuration, terrain and line of sight. Specifications sourced from Cambium Networks data sheets.



iStock.com/Chababla

From emergency vehicle to mobile command centre

Why connectivity is the backbone of modern emergency fleets

For today's police, fire and ambulance leaders, operations are being fundamentally reshaped by real-time data, distributed decision-making and the growing expectation of always-on situational awareness. Incidents are no longer managed from a single control room — they are coordinated dynamically across people, systems and locations, as situations evolve in real time. In that environment, the vehicle is no longer just how you get to the scene. Increasingly, it is a rolling command hub where decisions are made, intelligence is gathered and safety is actively managed in the moment.

Dash-mounted cameras are now AI-enabled plate readers, constantly scanning for stolen vehicles, wanted offenders and missing persons while officers focus on driving and tactics. Live video and rich telematics flow back to command, giving control rooms the same view as the personnel on the street. Route guidance is an intelligent system

that responds to congestion, hazards and evolving incidents.

All of this depends on one thing that is easy to overlook until it fails: resilient, intelligently managed wide-area connectivity and bandwidth into and from the vehicle.

This is where the combination of Axon's Fleet 3 in-car video and automated number plate reader (ANPR) solution and Ericsson's in-vehicle Wireless Wide Area Network (WAN) solutions comes together to create what operational leaders really need: a mobile extension of headquarters in every car, truck and fire appliance.

The new digital workload inside every vehicle

Consider what your frontline vehicles are being asked to support today:

- AI-assisted automatic number plate recognition (ANPR) scanning thousands of plates per shift, often across multiple lanes of fast-moving traffic.

- High-resolution dash-mounted, interior, and/or exterior video.
- Computer-aided dispatch (CAD), mapping and route optimisation that factors in live traffic and road closures.
- Sensors and telemetry for location, speed, door open/close, weapon lock status and more.
- Emerging use cases including drone integration, body-worn camera offload, and situational awareness platforms that draw on all the above.

Axon Fleet 3 was designed for exactly this environment. It brings mobile ANPR to every equipped vehicle, turning your fleet into a network of plate-reading cameras that can detect targets in a fraction of the time it would take manual checks. Dual-view cameras capture both the road ahead and the transport cabin with high resolution and infrared, delivering clear evidence day and night. Real-time awareness capabilities — including alerts, live maps and live streaming —

supervisors and operations centres a live window into unfolding incidents.

However, none of that intelligence exists or can be used if the underlying network connection drops just as a crucial alert is generated or a supervisor tries to view a live feed from a pursuit.

Why traditional vehicle connectivity is no longer enough

Many emergency services agencies still rely on legacy modems or a single-carrier data plan in their vehicles. These solutions were scoped for email, basic CAD messages and occasional database checks — not for continuous video, AI inferencing and cloud-based applications. This changing digital landscape means that today's emergency services risk profile looks like this:

- A single network outage or local cell issue can silently disable critical applications.
- Moving between coverage areas can introduce long reconnection delays.
- The vehicle's internal devices compete for the same limited bandwidth, leading to unpredictable performance.
- IT and radio teams have limited visibility into what is happening in the vehicle at the edge of the network, making troubleshooting slow and disruptive.

For emergency services leaders, this translates to field risk. An ANPR alert that fails to reach the officer, a map that freezes during a pursuit, or a live stream that drops in the middle of a high-risk stop are not simply 'technical issues' — they are safety issues for both officers and members of the public.

Building a resilient Wireless WAN for emergency fleets

Ericsson's in-vehicle Wireless WAN connectivity solutions are built specifically to solve these problems in public safety environments. The Ericsson Cradlepoint R980 and R2400 in-vehicle 5G routers are ruggedised devices designed for first responders and mission-critical fleets. They bring several capabilities that matter directly at the operational level:

- **Multi-carrier, resilient connectivity:** Dual-SIM and multi-link capabilities allow vehicles to use the best available carrier network and best connectivity source (e.g. cellular, satellite etc.) at any moment and fail over in milliseconds if one carrier has an issue. This keeps mission-critical applications online as vehicles move across jurisdictions and coverage zones.
- **High-performance, in-vehicle Wi-Fi:** Integrated, high-capacity Wi-Fi turns the

vehicle into a secure hotspot for all on-board systems — from Axon Body Cameras and Mobile Data Terminals to tablets and specialist equipment — without individual data plans for each device.

- **Precise location services:** Advanced positioning enables lane-level accuracy for tracking vehicles, assets and even drones, underpinning better dispatch decisions, geofencing and safety protocols.
- **Edge compute for AI and video:** Expanded on-device compute allows AI and video-processing tasks to run in the vehicle itself, reducing latency and keeping critical functions running even when backhaul bandwidth is constrained.

Layered on top of this, Ericsson's NetCloud management platform gives IT and communications teams a single pane of glass for configuration, security and monitoring across hundreds or even thousands of vehicles. This includes zero-trust security, SD-WAN and AIOps-driven analytics that can detect and often resolve issues before crews notice them.

Axon Fleet 3 plus Ericsson: a mobile extension of headquarters

When Axon Fleet 3 is deployed on top of Ericsson's in-vehicle Wireless WAN, the vehicle evolves into a fully integrated mobile node on a public safety network.

For a patrol supervisor, this means:

- ANPR hits detected by Fleet 3 can be delivered reliably and in real time, even when vehicles pass through coverage 'dark spots' or move between carrier footprints.
- High-definition video from either front-facing camera or interior camera that is monitoring transported people can be streamed live to the operations centre, giving tactical commanders the same view as officers on the ground during pursuits, critical incidents or public order events.
- Footage and metadata can be offloaded automatically, minimising manual intervention and reducing the risk of evidence gaps.

For communications and IT leaders, it means:

- Centralised, policy-driven control enabled with Ericsson NetCloud, over how video, ANPR, CAD and other applications share bandwidth — ensuring command-critical traffic is prioritised without starving other systems.
- Consistent security posture across the fleet, with encrypted tunnels from each vehicle back into the agency network, helping to protect sensitive evidence and operational data.

- The ability to deploy new cloud-based applications, firmware and security updates and configurations over the air, turning the vehicle into a platform that can evolve without repeated hardware swaps.

Ultimately, the combination of Axon's ecosystem and Ericsson's Wireless WAN allows your vehicles to function as genuine extensions of the command centre: aware, connected and ready to act as the incident evolves.

Preparing your fleet for the next decade

The digital workload on public safety vehicles will only increase. AI tools, real-time video analytics, connected drones, advanced mapping and sensor-sharing between agencies are rapidly moving from pilots to everyday practice globally.

Operational leaders who view connectivity as core infrastructure — not a commodity add-on — will be better positioned to:

- Shorten response and resolution times by getting the right intelligence to the right people at the right moment
- Increase responder safety through richer situational awareness and more reliable communications
- Strengthen community trust with better transparency, evidence handling and post-incident review.

By pairing Axon Fleet 3's advanced in-car video and ANPR capabilities with Ericsson's resilient in-vehicle Wireless WAN and NetCloud management platform, agencies can turn every emergency vehicle into what it was always meant to be in the digital age: a mobile, always-on extension of public safety headquarters.

Moving forward, the agencies that treat connectivity and connected technologies as core operational infrastructure — not simply a vehicle add-on — will be best positioned to deliver faster, safer and more informed responses in an increasingly complex operating environment.



**Ericsson Enterprise Wireless Solutions
Australia Pty Ltd**
cradlepoint.ericsson.com



IS YOUR AGENCY TRULY READY FOR AI IN PUBLIC SAFETY?

Chris Leaver, Executive Director – Australia & New Zealand, Octave

Al is already changing what it means to run an emergency communications centre (ECC). With AI for public safety already upon us, it's vital to best leverage it in ways that protect trust, support staff and improve outcomes.

Today, emergency communications are no longer limited to traditional voice calls. Requests for help are increasingly coming through multiple channels, which changes the workflow inside the ECC. It also changes what the centre needs from its broader ecosystem, as demand arrives through more sources with less time to separate critical information from background noise.

Moving beyond standalone tools

One of the biggest misconceptions about AI is that it can be added as a single feature or bolt-on solution. In practice, AI for public safety delivers the most value when it is integrated into the tools, data and workflows ECCs already use.

For example, during a major storm, an ECC may be flooded with calls about power outages, trees down, alarms and traffic issues. At the same time, other departments such as parks or utilities need timely information to respond, while neighbouring agencies may need situational awareness or mutual aid coordination. Not every request requires a phone call to a

call taker, but every request still needs to be managed accurately and efficiently.

When AI is part of an integrated environment, information can be routed to the right organisation at the right time, reducing unnecessary call volume and allowing telecommunicators to focus on true emergencies.

In this context, AI for public safety is less about automation for its own sake and more about improving how ECCs manage demand across the entire ecosystem.

Starting with practical use cases

For agencies early in their AI journeys, the most effective starting point is often



IN PRACTICE, AI FOR PUBLIC SAFETY DELIVERS THE MOST VALUE WHEN IT IS INTEGRATED INTO THE TOOLS, DATA AND WORKFLOWS ECCs ALREADY USE.

the simplest one. Focus on use cases that reduce friction without changing the core role of the ECC.

Language translation is one example: when callers and telecommunicators do not share a common language, delays can have serious consequences. AI-supported translation can help ensure critical information is exchanged quickly while keeping human judgment firmly in control.

Transcription and dictation also offer another clear benefit. Automatically converting calls and radio traffic into searchable text reduces administrative burden, improves documentation quality and creates data that can be used for training, review and analysis.

Quality assurance (QA) is another area where AI for public safety can make an immediate difference. Many ECCs are limited in how many calls they can review. AI-supported QA enables teams to evaluate a larger portion of interactions, identify trends and provide targeted coaching without adding staff hours.

These types of applications build confidence and trust while laying the groundwork for more advanced capabilities.

Extending value beyond the ECC

AI becomes even more powerful when it supports coordination beyond the ECC itself. Public safety incidents rarely exist in isolation. They often involve multiple agencies, departments and systems working together under time pressure.

AI for public safety can help ECCs share relevant information with emergency management, utilities, public works and neighbouring jurisdictions in a more timely and consistent way. It can surface relationships across data sources, highlight priorities and push updates to the people who need them most. The result is better coordination, faster decisions and fewer gaps during complex incidents.

This shift is especially important as agencies work to break down silos and move towards more collaborative operating models.

Asking the right questions early

AI adoption is not one size fits all: what works for one community may not be right for another — at least not yet — which makes evaluation critical.

Agencies should ask vendors where solutions are already deployed, what lessons have been learned and how those solutions fit the realities of public safety operations. It is also important to understand how AI capabilities will evolve over time and how performance will be monitored as conditions change.

Integration should be a central consideration. AI for public safety delivers the greatest value when it can work across trusted data sources rather than becoming another disconnected system.

Keeping people at the centre

AI brings both opportunity and responsibility. Data privacy, security, bias and accuracy must be addressed deliberately, especially in mission-critical environments. AI is not perfect and should never be treated as a final decision-maker.

Successful implementations keep humans firmly in control, using AI for public safety to support faster insight and better awareness while maintaining accountability and judgment where it matters most. When framed this way, AI becomes a tool that strengthens trust rather than undermining it.

A practical next step

For ECC leaders building an AI roadmap, the path forward starts with clear priorities, thoughtful integration and a focus on outcomes. Faster call handling, clearer information flow, better coordination and stronger support for personnel should guide every decision.



Dual-mode LTE Wi-Fi push-to-talk radio

The IP510H is Icom's latest push-to-talk handheld radio, combining 4G LTE and Wi-Fi connectivity in a single device to support wide-area communication with improved indoor coverage.

Designed for operational environments, the IP510H enables users to maintain communication across both outdoor LTE networks and indoor Wi-Fi coverage areas, helping to address common coverage challenges. Traditional two-way radios have to wait for the other party to finish speaking before taking turns, resulting in a large time lag between calls.

The IP510H supports IEEE802.11 a/b/g/n/ac Wi-Fi with WPA3 Enterprise/Personal security, while built-in Bluetooth supports cable-free operation.

The unit is compact and lightweight at 59.7 x 144.7 x 34.9 mm and 220 g, and is water and dust resistant to IP67.

With simple radio-style operation and dual connectivity, the IP510H provides a practical communication solution for industries such as transport, security, and field services.

Icom Australia Pty Ltd
www.icom-australia.com



Rugged Windows 11 tablets

Getac has announced the expansion of its ZX80 range of 8-inch fully rugged tablets with the launch of the ZX80W and ZX80W-EX Windows 11 devices built on ARM architecture.

The ZX80W and ZX80W-EX both utilise Qualcomm's QCS6490 platform, built on ARM architecture, for high energy efficiency and high performance-per-watt. Both devices also feature 12 GB of inbuilt LPDDR5 memory and 256 GB of universal flash storage.

By leveraging ARM's high thermal and energy efficiency, the ZX80W runs Windows 11 IoT Enterprise LTSC in a compact, fanless chassis.

The ZX80W and ZX80W-EX also feature a 6th Generation Qualcomm AI Engine to unlock real-time intelligence at the edge, reducing cloud dependency for faster, more reliable processing when an internet connection is patchy or unavailable.

Both devices are MIL-STD-810H and IP67 certified, vibration and 1.8 m drop resistant, feature a daylight-readable display, and have a wide operating temperature range of -29 to +63°C for the ZX80W and -21 to 55°C for the ZX80W-EX. Both are lightweight with the ZX80W weighing 590 g and the ZX80W-EX weighing 780 g.

In addition, the ZX80W-EX is also ATEX/IECEx Zone 2/22 certified for operator safety in hazardous and/or potentially explosive environments.

Getac Technology Corp

www.getac.com

EMC • EMR • RADIO • SAFETY • ENV

Accredited testing and global product approvals since 1992



EMC Technologies Pty Ltd

Melbourne: +61 3 9365 1000

Sydney: +61 2 9624 2777

Bayswater: +61 3 9761 5888

Auckland (NZ): +64 9 360 0862

www.emctech.com.au

Industrial radio modem

SATEL has released the SATEL-EASy+ ETH, the latest generation of its 403-473 MHz UHF radio modem for industrial wireless data networks.

The SATEL-EASy+ ETH provides Ethernet, Bluetooth v4.2 and USB 2.0 interfaces operating simultaneously. Data received on the radio interface is transmitted via all configured ports concurrently.

The Ethernet port supports 10/100 Mbps IPv4, DHCP client, TCP/UDP and ICMP, with a dual IP port structure separating system data from diagnostics. The unit is optimised for Modbus and supports SCADA and PLC communication. SATEL Source Routing, NMS Routing and TX/RX addressing enable large, flexible networks with over-the-air configuration.

Compatible with PacCrest, TrimTalk and RTCM-SC135 protocols, the SATEL-EASy+ ETH supports AES128 encryption as standard with AES256 via a DRM upgrade.

Rojone Pty Ltd

www.rojone.com.au



Tactical L+S band antenna

The Benelec Tactical FlexNek L+S band antenna is engineered specifically for modern battlefield environments, giving dual-band coverage tailored for handheld tactical radios, mobile ad-hoc networks (MANET), and unmanned systems (UAVs/UGVs).

The dual-band spectrum design offers continuous coverage across the 0.9 to 3.0 GHz frequency range with a stable 2.5 dBi gain for reliable long-range signal propagation.

Measuring 260 mm in total length, the compact design minimises snag hazards during operations, and the ruggedised flexible neck allows operators to bend and position the antenna up to 90 degrees to maintain polarisation or clear tactical gear.

The antenna is built to withstand extreme environmental conditions, and is fully compatible with the latest high-data-rate software-defined radios (SDRs) used in drone surveillance, encrypted team communications and real-time data streaming.

Benelec Pty Ltd

www.benelec.au



One network, one device

How MCPTx is replacing the two-radio problem



For decades, workers in hazardous industrial environments have carried two communication devices: a VHF or UHF radio for site communications, and a mobile phone for everything else. That duplication carries a cost: separate infrastructure, separate maintenance contracts, separate training programmes and separate failure points. The IS380.1 from i.safe MOBILE addresses this directly.

Certified for Zone 1 and Zone 21 and soon coal mining

The IS380.1 carries ATEX and IECEx certification for Zone 1 and Zone 21 hazardous areas. This means it is approved for use where explosive gas or combustible dust atmospheres are present during normal operation. The IS380.M1, a dedicated mining version of the device designed specifically for underground and surface mining applications, will be available soon.

Target sectors include utilities infrastructure, water treatment plants, mining operations, chemical processing facilities and defence logistics depots. The device runs ISM-OS 16, i.safe MOBILE's own operating system based on Android. It supports 2G, 3G and 4G networks and is rated to IP68 and MIL-STD 810H. The hardware is purpose-built for shift work in demanding environments, not a consumer device with a protective case.

3GPP-compliant MCPTx communication

The IS380.1 supports MCPTx communication compliant with the 3GPP standard — the internationally recognised framework for mission-critical voice, video and data over LTE and 5G. Unlike commercial PTT-over-cellular solutions, 3GPP-compliant MCPTx delivers network-level prioritisation, dedicated emergency channels, end-to-end encryption and full dispatch functionality. This ensures the IS380.1 meets the requirements of organisations where communication failure is not an option: emergency services, utilities, defence and

industrial facilities in hazardous areas. The device is also future-ready, with a clear migration path from LTE to 5G as network infrastructure evolves.

MCPTx versus VHF: what changes in practice

Mission Critical Push-to-Talk (MCPTx) over LTE delivers capabilities that conventional VHF simply cannot match. Group calls, individual calls, dispatcher interfaces and priority queuing all operate over a single broadband bearer. Coverage extends wherever 4G is available, rather than being constrained by the reach of a licensed repeater network.

For organisations that manage their own PMR infrastructure, the operational savings are significant. A single cellular PTT network replaces two parallel systems. Spectrum licensing, repeater maintenance and radio programming cycles can be reduced or eliminated. IT and comms teams manage one platform rather than two.

Organisations that are not ready for a full cutover have a practical migration path. The IS380.1 connects to third-party radio-over-IP gateways, allowing LTE users and legacy VHF users to speak on the same channel. Field teams on the IS380.1 communicate directly with colleagues still using conventional radios. The transition happens at the organisation's pace, without forcing simultaneous fleet replacement.

The connected worker in critical industries

Modern workforce management increasingly depends on data, not just voice. Lone worker protection, GPS tracking, digital permits to work, and real-time asset management all require a device that can run applications, not just transmit audio. The IS380.1 ships with the i.safe MOBILE App World pre-installed. This curated application

platform, hosted on German servers, provides access to validated software tested against the actual device hardware. PTT applications, lone worker protection, mobile device management and maintenance tools are available through a single controlled environment. Broadband PTT solutions built on this platform support features that go well beyond voice: video streaming from the field, image capture for incident reporting and integration with control room software all become possible on the same device the worker already carries.

Familiar to anyone who has held a radio

Radio engineers and comms managers know that the biggest resistance to any new device comes from the field. Workers who rely on communication in safety-critical situations do not welcome change for its own sake.

The IS380.1 is designed around this reality. The large side-mounted PTT button sits exactly where a radio user expects it. A programmable rotary switch handles channel selection or volume without looking at the screen. The front-facing amplified loudspeaker performs in high-noise environments. A 13-pin ISM interface maintains full compatibility with existing professional headsets. The replaceable battery supports continuous operation across long shifts without returning to a charging station.

The IS380.1 will be available through i.safe MOBILE's global distribution network, including the Australian subsidiary. Full technical specifications and supported PTT applications are at www.isafe-mobile.com.



i.safe MOBILE Australia Pty Ltd
www.isafe-mobile.com/en

Future-proofing RNZ's infrastructure

Radio New Zealand (RNZ) recently successfully replaced two aging AM broadcast masts with one new mast at the Henderson transmission site, securing Auckland's emergency broadcasting capability for the next generation.

State-owned telecommunications company Kordia played a major role in the project with the design of the new mast, development of the works methodology and the rigging works onsite.

RNZ's Henderson transmission site had long been the backbone of AM broadcasting for the wider Auckland region, carrying AM radio services from two aging masts: a 122-metre structure over 90 years old, and a 153-metre mast dating back more than 70 years.

The challenges were significant. The proximity of high voltage powerlines, critical underground services, transmitter building, roads and the Northwestern Motorway limited the methodologies that could be used for the works. The ground condition on the two sites required specialist crane access track and hardstand engineering, and trees on boundary areas created consenting complications that took months to resolve. Throughout the project, RNZ's AM services, including its emergency broadcasting function, had to remain available with minimal disruption.

Kordia's structural engineering and specialist rigging teams developed a comprehensive plan to decommission both masts and install a new 110-metre replacement, the height being determined by RNZ's AM operating frequency requirements.

The design drew on proven methodology from a prior Kordia mast project at Porirua's Titahi Bay, adapted for Henderson's unique site constraints. The new mast was engineered with a minimum 50-year design life.

Constructed in 6 m sections for transport efficiency, the mast was assembled by Kordia riggers into four larger sections onsite before crane installation. Each section required temporary and permanent guy wire installation before the next could be lifted into place.

Removing the 153 m southern mast presented a distinct engineering challenge. With hook heights beyond crane reach for the upper portion, and space constraints preventing ground-level operations, the top 40 metres required helicopter removal. Sections were cut to weigh no more than 800 kg — well within safe lifting limits — and the helicopter navigated between guy wires to place each section within the restricted site area.

Service continuity was built into the project from the outset, with careful management of outage windows. Emergency broadcasting protocols were established to halt work and restore services immediately if critical announcements were required.

Mast preparation works commenced in January 2026, followed by civil works ahead of the mast works which commenced on 16 April. On 12 May, the first AM services on the new 110 m mast were brought into service.



RNZ's Transmission Manager Steve White said the project pushed the boundaries of practical engineering, supporting eight AM radio services from a single mast, and was one of the most complex he has led during his time at RNZ. Internationally, it's rare to run this many AM services from one mast, with most networks opting to build additional structures instead.

"Replacing infrastructure that has served Auckland for generations while maintaining uninterrupted emergency broadcasting capability was a significant undertaking," he said. "The level of planning, technical expertise and collaboration between RNZ and Kordia was exceptional. The result is a modern, resilient transmission asset that will support our audiences and public service responsibilities for decades to come."

The new mast also secures Auckland's AM emergency broadcasting capability with infrastructure designed to last 50 years or more, directly supporting RNZ's critical public service role.

Kordia says the project stands as a benchmark for complex broadcast infrastructure renewal in constrained urban environments, combining specialist structural engineering, precision rigging, helicopter operations, multi-stakeholder coordination and live-service continuity management into a single, seamlessly delivered outcome.

RNZ Chief Technology Officer Mark Bullen says the project represents an important investment in RNZ's long-term resilience.

"This project is about much more than replacing aging infrastructure. It strengthens RNZ's ability to deliver trusted information when New Zealanders need it most, particularly during emergencies," he said. "The new Henderson mast provides a future-proof foundation for our AM broadcasting services and demonstrates what can be achieved through strong partnership, innovation and engineering excellence."

Kordia Limited
www.kordia.co.nz



iStock.com/Dragos Condrea

LEVERAGING BODY WORN CAMERAS IN RETAIL

A NEW LAYER OF SAFETY AND SECURITY

Axon Public Safety Australia

Body-worn cameras are not only a powerful tool for safety within retail settings, but can be viewed as a piece of a larger safety toolkit.

In recent years, retail stores have experienced a notable increase in theft and aggressive behaviour towards staff. Traditional security measures, such as CCTV systems, can make a difference but have shown limitations in directly preventing incidents due to their passive nature and distant positioning from potential perpetrators.

Across the globe, however, body-worn cameras (BWCs) have been shown to be an effective tool in a variety of contexts with respect to de-escalating situations and preventing aggressive behaviour. Law enforcement has been leveraging this technology for over a decade. For instance, a 2012 study showed officers in Rialto, California using BWCs were less likely to use force and experienced a significant drop in complaints. Multiple meta-analyses since then indicate that BWCs generally yield positive outcomes for police departments.

In an effort to continue evaluating the efficacy of BWCs in the retail environment, Adrian Beck recently ran a study with 16 participants.¹

Below are the four main reasons that retailers are considering the use of body-worn cameras.

Four main reasons for investing in body-worn cameras

1. Body-worn cameras act as a highly visible tool for deterring perpetrators and de-escalating incidents

As highlighted by Beck, public self-awareness serves as one of the strongest cases for BWCs. In a retail context where BWCs are involved, both sides of the interaction are aware that a camera is capturing current behaviour. The data suggests this is likely to result in eased tensions because the proximity of the camera promotes greater accountability.

To support this point, one respondent in the study shared a specific incident.

»

"We had an example in [name of store] where a customer was trying to get a refund and began swearing at the staff. She then saw the camera and walked away," the respondent reported. "A little later she returned to apologise, and staff had never seen this before and believe it was because of the camera. People don't want to end up on TV and they think it played on her mind to the point where she came back and apologised."

2. Body-worn cameras provide reassurance and support to employees

Beck's study found that 66–80% of staff felt safer because of the introduction of BWCs. This has helped retailers feel more confident when it comes to intervening during suspicious situations.

One respondent explained it by saying "some [staff] said that when wearing the camera, they were more likely to intervene when they saw something suspicious and have greater confidence when dealing with an incident because they know their actions are being recorded and offenders cannot misconstrue what has occurred..."

3. Body-worn cameras gather sharable evidence on offenders and a record of what occurred

While participants in the study indicated that BWCs' ability to serve as a proactive de-escalation tool is a compelling reason for deployment, this technology still has extreme benefit when de-escalation is not possible.

Retail staff will encounter different types of perpetrators; professional thieves or disruptive customers suffering from substance abuse or mental health issues are often undeterred by the notion of being recorded. Therefore, BWCs serve as an important evidence collection mechanism, and that evidence plays an important role in ongoing staff safety, police investigations and for prosecution.

4. Body-worn cameras positively influence the behaviour of those wearing the devices

While some respondents in the study noted this is more of a marginal benefit, others noted it did mediate the behaviour of wearers in a positive way, particularly those who are security staff.

One respondent in the study mentioned that: "What we have seen is that staff have admitted that it does change how they behave because they know they are on camera as well; it has moderated their behaviour."

The key is to educate wearers on how footage can potentially be used as evidence; therefore, thorough training on appropriate behaviour when responding to an incident is critical.

Deployment of body-worn cameras

Overall, Beck's study found that there is no one-size-fits-all approach to implementing this technology in a retail setting. Developing clear guidelines about when and where to use BWCs is beneficial for staff in order for them to be most effective. For example, staff must be aware that body-worn cameras won't be used to monitor performance or be active in bathrooms and that adoption is solely in the interest of staff safety.

Ultimately, management must determine the best practices and policies to facilitate buy-in and drive better safety outcomes by utilising BWC technology. Respondents in the study provided insightful qualitative and quantitative data that suggests BWCs are not only a powerful tool within retail settings, but can be viewed as a piece of a larger safety 'toolkit' when leveraged in conjunction with CCTV, SOC's and other approaches.

1. Beck A 2024, *Body Worn Cameras in Retailing: A Review of Use and Impact*, Beck Research and Consultancy Ltd, <https://www.axon.com/resources/body-worn-cameras-in-retailing>

Mobile 5G router

Designed for vehicles and mobile field teams, Ericsson Cradlepoint R2400 mobile 5G router combines ultra-fast failover, precise location services and edge computing to help organisations operate safely, efficiently, and with confidence.

Compatible with public safety networks and new network slicing services, the R2400 leverages the latest in 5G standalone Release 17 technology to support increased capabilities across public safety, mass transit and private fleet networks.

The R2400 offers fast carrier failover with Dual-SIM/Dual Standby (DSDS) on a single modem that enables carrier switchover roughly 10 times faster, keeping voice, video and data flowing during critical missions and transit routes.

Centimetre-level location accuracy through real-time kinematics (RTK) combined with dead-reckoning improves positioning from 1–3 m to approximately 1 cm, enabling lane-level vehicle identification and precise real-time tracking of personnel, assets and drones, while multi-link resiliency — through support for up to five simultaneous cellular plus multiple low-Earth-orbit (LEO) satellite connections — maximises throughput and availability.

It also offers improved in-vehicle Wi-Fi through an embedded software-defined Wi-Fi 7 access point that delivers approximately 2–4 times faster Wi-Fi speeds for passenger and operational communications across mass transit and public safety.

Edge computing has been expanded with increased power to support local AI inferencing, computer vision, and to support enhanced performance for containerised applications, while faster security processing allows support for NetCloud SASE's zero-trust security and SD-WAN services to provide a highly secure and optimised WAN network across fleets, sites and critical assets.

Ericsson Enterprise Wireless Solutions Australia Pty Ltd
cradlepoint.ericsson.com





Direction-finding receiver

The R&S PR300 is a portable monitoring and direction-finding receiver from Rohde & Schwarz with 125 MHz real-time bandwidth and high-speed scanning of more than 500 GHz/s. The device has been specifically engineered to cope with the increasing demand for greater bandwidth and signal quality in the modern electromagnetic spectrum.

The PR300 expands the real-time bandwidth available to keep pace with cellular technology as it trends towards higher bandwidths, which current high-data-rate applications require. The PR300 is designed to provide detection of complex wideband signals in unknown signal environments with 125 MHz real-time bandwidth and high-performance preselection.

Advanced features designed for field efficiency, such as segmented panorama scan, embedded spectrum analysis functions, and direction finding (DF) on time-gated signals, are included. Despite its portable size, the PR300 offers a frequency range from 8 kHz to 8 GHz, time domain analysis, and I/Q recording and analysis.

The tool is designed for a broad range of applications, ranging from radio monitoring measurements in line with ITU recommendations for civil authorities, ensuring quality of service (QoS) for network operators, along with military and intelligence applications. The PR300 is compatible with existing R&S handheld antennas and compact DF antennas.

Rohde & Schwarz (Australia) Pty Ltd
www.rohde-schwarz.com.au

The RFUANZ Gala Dinner and Awards recently returned to the North Island for the first time in several years. Industry leaders, innovators and professionals gathered at Te Papa in Wellington on 27 May for an evening of celebration and recognition. The change of location brought a fresh energy to the event, attracting strong attendance

from across New Zealand's radio communications sector and providing an excellent opportunity for networking, reconnecting with colleagues, and acknowledging the outstanding achievements that continue to drive the industry forward.

The evening commenced with an address from Communications Minister Paul Goldsmith, who spoke about the critical role communications infrastructure plays. He acknowledged the importance of reliable communications networks and reaffirmed the government's commitment to supporting growth and investment within the communications industry. His message reinforced the significance of the sector and the work being undertaken by organisations throughout New Zealand to ensure communities remain connected.

One of the highlights of the evening was the presentation by renowned mountaineer and adventurer Mark Inglis, who also served as Master of Ceremonies. Mark captivated the audience with his inspiring account of mountaineering experiences on Aoraki / Mount Cook and the challenges he faced during a 13-day snow blizzard. His story highlighted the importance of resilience, teamwork, determination and the vital role that radio communications played when help was needed. His recollections of using radio communications to seek assistance during extreme conditions provided a powerful reminder of how critical reliable communications can be in life-threatening situations. Mark's storytelling and inspirational outlook ensured his presentation was one of the most memorable aspects of the evening.

The awards ceremony recognised some of the industry's most deserving individuals and organisations. Laurie Colvin of Colvin Communications received the Lifetime Service Award, while the Project Excellence Award was given to Chris Prouse and Leyton Smith (Dove Communications and Whakatāne Radio Association of New Zealand).

Crystal Shuttleworth of Mount Campbell Communications received the Health and Safety Award, while the Young Achiever Award was won by Nissa Absalom of Tait Communications, and the Local legend Award by Blair Hopkins of Ashley Communications.

Congratulations to all winners.

The success of the evening was made possible through the generous support of our event sponsors. Special thanks go to Platinum Sponsor Tait Communications, with CEO Yoram Benit addressing attendees and sharing insights into the future of the communications sector.

Thanks also to our Gold Sponsor Go WiFi, and Silver Sponsors Ashley Communications, Cambium Networks, Dove Communications, Logic Technologies and Outback Communications.

A sincere thank you also goes to Westwick-Farrow Media for delivering another outstanding Comms Connect event and to our industry partner ARCIA for their continued support and collaboration.



The RFUANZ Gala Dinner and Awards once again showcased the talent, innovation and dedication that exists throughout New Zealand's radio communications industry. With the event's successful return to the North Island, attendees left Te Papa reflecting on a memorable evening and looking forward to the opportunities and achievements that lie ahead.

Mikaela Robinson
Events Manager, RFUANZ



Port Nelson deploys private 5G network

A key gateway to the South Island, Port Nelson underpins New Zealand's economy, handling a diverse range of exports and imports, including forestry products, pip fruit, wine and seafood. Within its warehouses, where palletised bottled wine and empty wine bottles move in and out of the port, forklift operators are required to scan every pallet moved as part of critical inventory and logistics processes. However, the high-density block-stacking storage used in these warehouses — and the complex design of the broader port site — had created persistent Wi-Fi dead spots and forced staff to change operating processes simply to maintain connectivity.

"Connectivity was becoming a real operational constraint for us," said Reagan Pattison, General Manager Business Transformation at Port Nelson. "No matter how much we tried to saturate our warehouses with Wi-Fi, we couldn't get consistent performance. That impacted productivity, created frustration for our operators, and limited our ability to modernise how we work."

Covering around 30,000 m² across three warehouses in Nelson and Blenheim, Spark's 5G+ Private Network solution uses Ericsson Private 5G to provide a high-availability core at Port Nelson that connects to small cell radios to provide reliable coverage inside the warehouses and across outdoor yard areas. The Port has also deployed Ericsson Cradlepoint ruggedised R1900 routers for forklift connectivity and tracking. The dual-SIM capability of the routers enables switching between Spark's public and private 5G networks for when forklifts move outside the initial private 5G coverage areas.

Unlike traditional Wi-Fi, private 5G delivers dedicated, secure, enterprise-grade connectivity with predictable performance and pervasive coverage across complex sites like the port, enabling staff to scan pallets in real time without interruption as they move throughout the sites.

In addition to immediate productivity and staff satisfaction gains, Ericsson's NetCloud platform gives Port Nelson improved visibility into connectivity performance, helping teams proactively identify and resolve issues.

A digital push-to-talk communications platform, enabled by Ericsson Private 5G, will play a key role in strengthening health and safety outcomes by improving real-time communications and enabling location-based alerts to help physically separate people from heavy mobile plant. Future applications include geofence intelligence and broadcast messaging.

"Safety is fundamental in a port environment. Private 5G gives us the ability to prioritise critical communications, improve visibility of what's happening across the site, and move towards more proactive, engineered safety controls," Pattison said.



"In a warehousing environment where there are moving vehicles and large volumes of stock moving in and out of the space, reliable connectivity that digital workflows can depend on really matters," said Ian Ross, Head of Private Networks ANZ, Ericsson Enterprise Wireless Solutions. "Private 5G is the digital backbone of modern industry, increasingly demonstrating the highest standard when it comes to connectivity for critical applications in factories, warehouses, airports, mines and ports."

"By using Private 5G, Port Nelson now has a dedicated network using the latest cellular wireless capabilities, that can support real-time operations today while providing a strong foundation for future digital innovation."

"Port Nelson is a great example of how private 5G is unlocking new value for New Zealand businesses operating in complex, production-critical environments," said Greg Clark, Chief Customer Officer at Spark. "At Port Nelson, it's enabling safer warehouse operations today while opening the door to automation, advanced IoT, and smarter ways of working across the entire port in the future."

Looking ahead, the port's warehouse private 5G network has the potential to further transform its operations by enabling advanced applications such as real-time asset tracking, predictive maintenance, enhanced CCTV cameras, AI-enabled vision and automation — delivering ongoing improvements in both productivity, and health and safety outcomes.

By strengthening the reliability and efficiency of a critical export gateway, the private 5G network delivered by Spark and Ericsson has the potential to unlock productivity gains for Port Nelson, the wider South Island, and the region's economy.

Ericsson Enterprise Wireless Solutions Australia Pty Ltd
cradlepoint.ericsson.com

HOW THOUSANDS OF TINY DOTS COULD SAVE FIRST RESPONDERS' LIVES

Gary Howarth

In an emergency, knowing exactly where a first responder is can mean the difference between life and death. When a firefighter in a burning building fails to check in, how does the commander know where to look for them?

Public safety agencies face daily challenges in finding first responders inside large buildings. Yet there are no reliable methods for tracking first responders in these types of environments.

To try to solve this problem the US National Institute of Standards and Technology (NIST) partnered with Indiana University's RedLab. The goal of the First Responder Smart Tracking (FRST) Challenge was to create prototype devices that track first responders indoors. In the five years since the challenge launched, teams from across the world have developed dozens of novel solutions — some of which have been turned into commercial products.

NIST is working with teams to ensure that their solutions meet the needs of public safety agencies, such as encouraging participants to make products affordable enough for first responder budgets.

GPS and the challenge of indoor navigation

The widespread adoption of GPS has mostly solved the difficulty of navigating outdoors, but GPS is unreliable indoors. Tracking our location with GPS requires a device to sense signals from satellites surrounding the user's location, but layers of building material can block or interfere with those signals.

This problem is even worse for high-rise buildings. They have more building material and are often built in dense urban environments. In these scenarios, it's even more critical for an incident commander to know exactly where their personnel are located.

The FRST Challenge asks participants to create wearable devices that are:

- easy to wear and carry
- able to track a responder accurately through complex buildings and long paths
- capable of communicating back to the base station
- tough enough to survive a firefighting environment.

The challenge

Verifying the accuracy of these systems is a significant challenge. That's why NIST used the dots facility, an indoor localisation test bed developed by Nader Moayeri on the NIST campus in Gaithersburg, Maryland, to test these systems.

This system involves more than 2000 carefully documented points (marked with stickers) inside and outside NIST buildings. These points, or 'the dots', are spread throughout the campus — in



One of the thousands of 'dots' on the NIST campus in Gaithersburg, Maryland, used as part of a challenge to test approaches to locating first responders.

hallways, stairwells, offices, laboratories, machine shops, underground tunnels, warehouses and many other spaces. The variety and size of locations available makes the NIST campus an ideal place to conduct these experiments.

In May 2025, NIST put the competitors' systems through their paces. Teams attached their systems to participants who navigated a series of scavenger-hunt-like missions. They had to find hundreds of individual points. Each team used its system to estimate the position of each dot along its course. NIST scientists and engineers then analysed the data against the known position of each dot to rigorously judge the accuracy of each system.

Continuing the research to keeping first responders safe

If first responders are going to use this technology, there has to be confidence in it and it has to be shown that it's been thoroughly tested.

Although the FRST Competition has officially wound down, NIST will continue to work with partners on developing indoor tracking innovations for first responders.

To that end, NIST recently built the Public Safety Immersive Test Center in Boulder, Colorado, to conduct research on first responder user experience and location-based service technologies. These researchers are also testing algorithms to track first responders in buildings.

Competitions such as this one encourage private sector innovations in public safety. Without them, companies wouldn't have the financial incentive to invest in creating these types of products.

Gary Howarth is a principal investigator for the mission-critical communications portfolio in the Public Safety Communications Research Division of the US National Institute of Standards and Technology (NIST). Gary earned his PhD in chemistry at Columbia University. He has previously taught high school science and co-founded a charter school in New Orleans.

Safer skies: advancing mining drone operations



For over a decade, Hancock Iron Ore's Roy Hill mine has leveraged drone technology to improve both efficiency and safety across its extensive mining operations. With the recent shift towards Beyond Visual Line of Sight (BVLOS) operations, Hancock Iron Ore required advanced airband communication solutions that comply with new Civil Aviation Safety Authority (CASA) regulations. These enhanced systems are vital for ensuring safe and effective long-distance drone flights, enabling detailed site monitoring and reducing the need for staff to operate in hazardous conditions.

The scale of the challenge was large. The Roy Hill mine is one of Australia's largest iron ore operations, with the mineral tenement stretching approximately 30 km. This extensive site features a conventional open-pit mining operation, processing plant, and heavy haul rail, sending around 64 million tonnes to customers annually.

Prioritising safety and operational efficiency, the implementation of BVLOS and smart, intelligent systems play a key role in achieving ongoing coordinated site management.

Icom's airband dealer, Aviassist, was approached to submit an application to CASA for licence approval. This collaboration with Aviassist enabled Roy Hill to implement the necessary airband communication systems, utilising the Icom IC-A120E VHF airband transceiver, the VE-PG4 RoLP gateway and IP100FS remote communicator, to meet both operational and regulatory standards.

In this set-up, there are three IP100FS remote communicators: two main units on PC control stations — one at the mine site and one in the Perth office — and another on a laptop used as a remote emergency

control station. This configuration allows operations to be managed from either the mine (while still outside the operational areas), the Remote Operations Centre (ROC) in Perth, or from a remote location during an emergency. The Spatial Solutions and Services team can remotely launch and control drone flights from the ROC as needed, streamlining operations and enabling real-time monitoring without the need to be physically present at the mine.

Icom's solution integrates the VE-PG4 gateway with the IC-A120E airband transceiver to support BVLOS operations by providing real-time communication for drone operators. This set-up ensures seamless contact with air traffic control (ATC) and internal teams while broadcasting the drone's location and flight details to nearby manned aircraft. This approach not only helps comply with aviation regulations but also prevents potential conflicts of airspace, enhancing both situational awareness and safety. By facilitating communication with regional ATC and maintaining internal communications, Icom's system supports effective emergency response and operational efficiency. Redundancy is also a priority, with an Icom IC-A16E airband handheld radio available as a back-up for staff members onsite.

The integration of Icom's airband communication system has improved real-time monitoring capabilities, enhancing efficiency and supporting ongoing safe operations at the Roy Hill mine.

Icom Australia Pty Ltd

www.icom-australia.com



How the World Communicates

Built Tough. Designed Smart. Future-proof.

VHF AND UHF DIGITAL TRANSCEIVERS

IC-F3600D VHF Model

IC-F4600D UHF Model

Series

ANGLED KNOB DESIGN

IP68 & MIL-STD-810 DURABILITY

AES/DES ENCRYPTION

ERGONOMIC,
GLOVE-FRIENDLY DESIGN

BLUETOOTH® CLASSIC & LE

USB TYPE-C® (PD) FAST CHARGING



*Night mode ON

iDAS NXDN™ IP68

ICOM DIGITAL ADVANCED SYSTEM

*Both VHF and UHF models are available in Simple Keypad and Full Keypad versions.



SCAN TO
LEARN MORE

www.icom.net.au

Hear the call. And hear everything else.

INNER CALM. SITUATIONAL AWARENESS.



CRS-1WLWTH
1 Wire Lightweight
Temple Headset
*2 Wire option
available*



CRS Temple Headsets combine discreet, lightweight comfort with bone conduction technology that keeps your ears open to the world around you.

Designed for professionals operating in high-awareness environments, they deliver clear, reliable comms without compromising situational awareness.

Ideal for security teams, logistics staff, warehouse operators and tactical applications, they help users stay connected and alert to everything around them, not just the conversations in their ears – or heads!

**When shutting out the
world isn't an option
insist on CRS!**

Phone 1300 307 334
www.crsaccessories.com.au



CRS
ACCESSORIES