WHITE PAPER

Comm Together: Unifying Your Critical Communications

EXECUTIVE SUMMARY

For the past decade, critical communications have been defined by digital land mobile radio (LMR) technologies TETRA, P25, and DMR; indeed mission critical voice and data services have been framed in terms of what LMR could deliver. Now we are told that LTE – and eventually 5G – will better meet the critical communications requirements of public safety, utilities, transport, mining and others; that while these technologies won't replace LMR overnight, replacement is inevitable and we must start planning now.

In this paper, we will investigate:

- Where are Critical Communications heading?
- What is changing the Critical Communications Market?
- Best of both worlds: 4G LTE *and* LMR
- Mission-critical LTE?
- Unifying your Critical Communications
- Developing UCC solutions for the real world

WHERE ARE CRITICAL COMMUNICATIONS HEADING?

Experienced network operators are all too aware of the associated costs and risks inherent in wholesale replacement of their communications network. Fortunately, there is an effective alternative, as Ross Spearman, Chief Technology Officer at Tait Communications explains:

“The future of comms… is really the convergence of voice and data over multiple bearers…to make that happen in a seamless way for the end user, so they don’t care what network they’re on: it just works”.

This is ‘Unified Critical Communications’ (UCC) – an approach that is both radical, and deceptively simple.

Unlike traditional reliance on a single communications technology, Unified Critical Communications combines the strengths of a diverse range of technologies, while mitigating their individual weaknesses. It will:

- replace traditional single-technology solutions with multiple communictions bearers,
- open up the choice of a much wider range of equipment types and vendors,
- integrate different networks so that they are managed as one,
- deliver communications to users who are unaware that they are using multiple networks,
- deliver critical communications as a service to frontline personnel.

DEFINING CRITICAL COMMUNICATIONS

Regardless of industry or organization, critical communications systems share these core requirements:

- High availability – communications services available without interruption
- Reliability – performance and coverage consistently meet required service levels
- Call services – at least voice calls (group, individual, priority), and data communications (short data services, packet data)
- Security communications services, access and critical information are protected
- Interoperability – for public safety, national security and military organizations, communications interoperation between organizations and networks (including different network types)

Critical communications systems must be able to deliver their services 24/7, including real-time group communications, manage intermittent heavy traffic loads, maintain communications in the face of damage or outages, and ensure the security of all communications. In contrast, consumer networks – designed to reach the largest number of subscribers with competitively priced service options – work within a ‘best effort’ model that cannot guarantee availability, reliability, or security.

WHAT IS CHANGING THE CRITICAL COMMUNICATIONS MARKET?

Increasing Market Size

The Critical Communications market is huge and growing rapidly – although there is a lack of consensus over exactly how big it is. Some analysts forecast the global value of Critical Communications reaching USD $20.12 billion by 2023, at a CAGR of 8.1% (up from a 2016 baseline of USD $11.76 billion). Others place it at around USD $10 billion by 2022, based on increasing integration of LTE and LMR.

Similarly, there are divergent views on market segment growth in the Critical Communications market. While some pundits see public safety taking half the market, IHS Markit views utilities as leading mission-critical LTE sales, followed by public safety, transportation and industrial.

Either way, it's a safe bet that Public Safety organizations continue to invest heavily in both LMR and LTE critical communications, with no indication that a transition from LMR to LTE is imminent.

Changing Expectations

It is useful to recap on how major changes in technology have shaped critical communications expectations, for both operators and users.

Mobile radio	LMR as starting point for critical comms: keeping personnel in touch.
Personal computing	Software replaces hardware functions and designs.
Networking	Distribution and integration of information. TCP/IP open standards start.
Open standards	Interoperability and commoditization of comms products.
Mobile phones	Consumer-grade cellular voice (and texting) competing with LMR.
Digital LMR	Development and roll-out of P25, TETRA, DMR open standards.
High bandwidth data	Fast, wide-area distribution of control and non-text data e.g. video.
Smart phones	Ubiquitous data-oriented cellular with better services and UI than LMR.
Automation	Faster and lower cost integrated control and operation.

Even before LTE, cellphones highlighted the contrast between what domestic consumers used, and mission-critical portable radios.

- Cellphones had become light-weight, pocket-friendly, easy to operate, with high res displays, alphanumeric keys, and a wide array of user applications. Heavily subsidized by telcos, they were also relatively inexpensive.
- On the other hand, LMR portables were big and heavy, expensive, with monochromatic displays, required training, and had almost no applications. But unlike cellular phones, LMR equipment was extremely rugged, with big batteries that gave it superior range, supported push-to-talk (PTT) talkgroup and individual voice calls, and communicated reliably across resilient networks that could handle peak loads without congestion or failure.

The game changer: high speed data

The introduction of high-speed data into communications was transformative. Until the beginning of the 21st century, critical communications systems were voice-oriented LMR, and – with the exception of text-oriented short data services – data was considered a nice-to-have. LMR narrowband data was limited to whatever could be pushed through a 9600 bps channel. With 2.5G, General Packet Radio Service (GPRS) could be grafted onto LMR, but data calls were charged by usage (bytes downloaded or duration).

When 3G appeared, the discrepancy between cellular and LMR widened into a chasm. 3G HSPA standards delivered data rates that could support Internet access, high-resolution graphics, video streaming, video calls and even internet TV.

Within a short time, both LMR companies and their critical communications customers recognized that narrowband data performance was holding back the improvement and expansion of their operations. However, when UCC combines the superior reliability and security of LMR with cellular high-speed data, it is a serious game changer.

Without sacrificing the trusted integrity of their mission critical communications, organizations can access features that might have seemed virtually unimaginable a decade ago.

Here's what to expect:

Law Enforcement

- Evidential-quality police video uploads, license plate recognition, vehicle database checks, gunshot location surveillance, real-time automatic vehicle location.

Fire

- Fireground video monitoring, GIS maps in real-time, physiological monitoring of firefighters.

EMS

- Remote coordination between ambulances and hospitals to monitor patients, including real-time medical telemetry (ECG, EEG), patient medical history and medical images.

Public Transport

- Fleet monitoring for rail and metro, wide-area Real Time Passenger Information (RTPI), traffic light pre-emption.

Mining, Oil and Gas

- Remote control and diagnosis of oil platforms, rigs, pipelines, power utility plants, and mine operations.

Utilities

- Next generation smart grid with distributed generation, real time demand forecasting, response and load balancing, full distribution automation, teleprotection, smart lighting, dynamic energy pricing.

BEST OF BOTH WOLRDS: 4G LTE AND LMR

With 4G LTE offering broadband data rates considerably better than 3G, the innovations promised for critical communications move from the theoretically possible to the practically and economically feasible. John Gorrell, Tait Vice President of Corporate Strategy points out:

> *"Public safety's appetite for situational awareness data, especially video, has accelerated thanks to the roll-out of national LTE networks such as FirstNet in the U.S., the Emergency Services Network (ESN) in the United Kingdom, and SafeNet in Korea."*

Does this mean the LMR is becoming irrelevant to public safety? It would seem not.

In fact, even the operators of these vast LTE systems warn that public safety agencies cannot rely on LTE alone. They consider LMR to be a necessary element of public safety critical communications for the foreseeable future.

For example, the official FirstNet website states:

> *"First responders currently use land mobile radio (LMR) networks for mission critical voice communications. When the nationwide public safety broadband network (NPSBN) is launched, it will not replace their LMR systems. The network is expected to initially transmit data, video, and other high-speed features, such as location information and streaming video, as well as non-mission critical voice. Public safety entities will continue to use LMR networks for their mission critical voice needs…*
>
> *… Public safety entities will continue to rely on their LMR networks for mission critical voice features – such as Group Communications and Direct-Mode – that are needed in an emergency response setting"*
>
> (Source: https://firstnet.gov/network/lmr)

One aspect of this emergency response setting needs emphasizing for all critical communications. LMR is consistently the last technology available when all others fail, due to a variety of failsafe options designed to preserve communications – even when major components of the network are damaged or become inoperable. Thus, if the core network in a multi-site LMR system fails, individual sites can switch to local standalone operation and connect any units within range. Even if all sites are down, units can still talk to each other in direct (simplex/talkaround) mode. Unique to LMR, these fallbacks are crucial for public safety.

Conversely, LTE was designed as a pure data network that gives the maximum number of customers the maximum service, data rates, and capacity on a 'best effort' basis. Voice has been added as push-to-talk over cellular (PoC) and voice-over-LTE (VoLTE), both of which convert voice to data for transmission, then re-converts at the other end into voice. Mission-critical public safety users require public safety grade (PSG) push-to-talk operation that far exceeds 'best effort':

> *"A PSG communications system should be designed to resist failures due to manmade or natural events as much as practical. This definition includes descriptions of coverage criteria for public safety systems that must be considered as a component of system reliability and elements of resiliency that ensure a rapid return to optimal performance….*
>
> *…PSG when applied to a public safety service or function (such as PTT) should focus upon what differentiates that service from a similar type commercial network supported service."*
>
> (Source: National Public Safety Telecommunications Council (NPSTC) 'Defining Public Safety Grade Systems and Facilities' Final Report 5/22/2014)

Until recently, public safety users trialing PTT over cellular (PoC) discovered that many versions fell far short of public safety grade and, if integrated with specific carriers, failed to work across systems. (This does not appear to be a problem for OTT versions of PoC such as EsChat which are independent of any carrier.)

NPSTC has laid out a number of specifications for public safety grade systems. including PTT. However, research has uncovered vulnerabilities in LTE networks, which could also slow the uptake for mission critical systems, until fundamental issues are addressed.

(See: https://arstechnica.com/information-technology/2018/03/even-more-bugs-in-lte-networks-allow-eavesdropping-fake-emergency-messages/)

MISSION-CRITICAL LTE?

LMR continues to be the technology that comes closest to meeting PSG specs, after decades of field and interoperability testing, customer experience, standards and product refinement. However, LTE is catching up fast, with mission-critical additions to LTE standards being implemented in LTE-A, that could potentially revolutionize communications for public safety as well as business.

Fifth Generation (5G) just around the corner

A game-changer in mobile communications, 5G is a key element of the rapidly-expanding Industrial Internet of Things. The objectives of 5G are a precise fit for critical communications users: support for more connectible devices, faster data, huge mobile data volumes, ultra-low latency, and better battery efficiency. Here's how 5G numbers stack up against 4G LTE:

	Latency	**Throughput**	**Connections**	**Mobility**
	end-to-end	*bps per connection*	*connections per km²*	*speed in km/h*
5G	1-10ms	1Gbps-10Gbps	1000K	500
4G LTE	30-50ms	100Mbps	10K	350

Standards organization 3GPP is undertaking an ambitious 5G standards plan, locking in 5G features for a smooth transition from LTE-A Pro. In other words, 5G is building upon LTE with new technologies to create massive capacity, ubiquitous mobile coverage, substantial performance advantages and network flexibility.

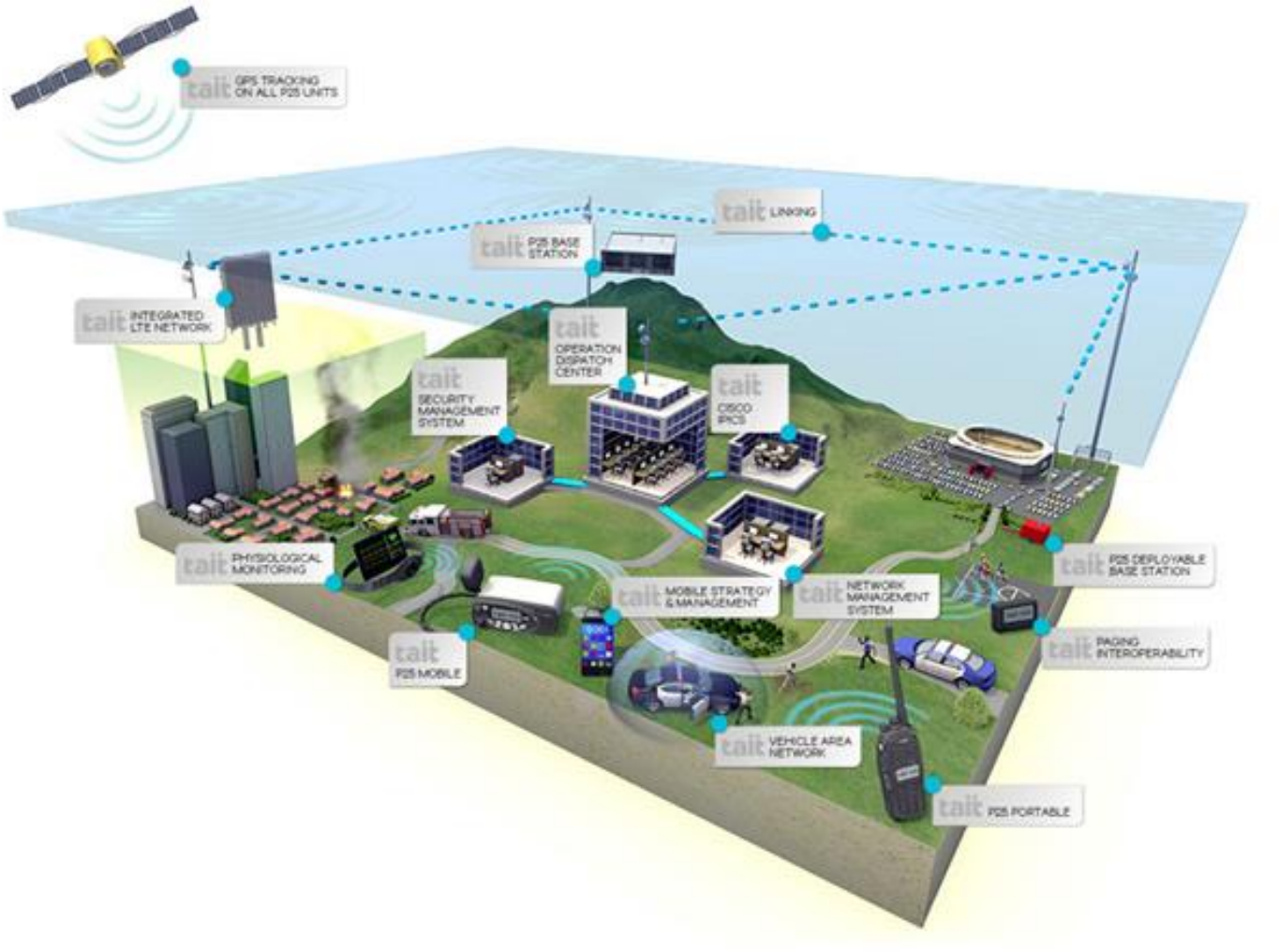
A completely redesigned radio air interface is already developed. 5G New Radio (5G NR), prototype equipment is being trialled, as well as undergoing interoperability testing with a radically-revised 5G RAN (radio access network). Nevertheless, as 3GPP has emphasized, it will be some years before 'full 5G' is delivered to the market, indicating 5G expansion features (including 5G Vehicle-to-Everything (V2X) and 5G Industrial IoT (5G IIoT)) are still work-in-progress.

These expansion features are all critical for machine-to-machine (M2M) communication, connected driverless vehicles, smart real-time AI-driven analysis, telepresence control, mobile computing, industrial VR and AR, robotics, and advanced automation that will transform business and society.

However, security remains a key concern for 5G. Dramatic increases in IoT-connected devices and sensors will increase risk, since many of these devices and networks carry unknown vulnerabilities because they were not designed with security in mind. While manufacturers will call on their experience in securing LTE systems, 5G is a different technology, and its security remains largely uncharted territory.

Nevertheless, one commentator recently described 5G potential:

> *"5G is intended to give the perception of 100% coverage as the quality, speed and predictability of the user experience will give the impression of full coverage, continuous availability and infinite capacity whether the user is at rest or on the move, wherever the user is or going to."*
>
> (Source: Sacha Kavanagh '5G vs 4G: No Contest' (September 27, 2018) https://5g.co.uk/guides/4g-versus-5g-what-will-the-next-generation-bring/)



UNIFYING YOUR CRITICAL COMMUNICATIONS (UCC)

Unified Critical Communications is not a new technology, but an innovative integration platform. Diverse products and communications methods (legacy, current and new) work together to present a consistent, unified user interface and experience. Voice, data, video, mobility, and presence services are seamlessly integrated across endpoints, devices, and applications via multiple bearers.

UCC amplifies the relative strengths – and counteracts the weaknesses – of each technology, to create a robust, resilient network of networks. In doing so, it overcomes the shortcomings of these common strategies:

- Investing in a new technology that promises to do everything is a considerable gamble. It requires a costly changeout of equipment, training, and processes, and risks that existing processes and systems may not work. Unlike smartphone consumers, critical communications operators cannot afford interruptions to their LTE communications
- Real-life integrations often do not go far enough, leading to a collection of communications subsystems that appear internally integrated, yet managed separately, and only loosely connected. Getting them to work together – coordinating overall performance, monitoring security, and administering consistent access control – is complex and costly.
- Integration through proprietary interfaces can severely constrain interoperability, locking organizations into buying only from vendors that support that proprietary connectivity.

Moving beyond those piecemeal integrations, UCC seamlessly integrates any combination of voice, data, text, images, or video. The system itself automatically selects the best network to deliver these quickly, reliably and securely across various devices, endpoints, and applications – without user input. UCC dynamically adopts the best delivery method available at that moment, whether it is LMR, WiFi, 3G/4G cellular, Private LTE, Satellite, etc. Endlessly flexible, UCC supports the most appropriate aspects of existing technologies while accommodating future developments such as 5G.

- **Increase Operating Efficiency**
  A Unified Critical Communications network can be configured to select the appropriate bearer for each communication, based on your criteria. You establish the priority – reliability, cost, power usage, timing, or availability – to meet your business requirements.
- **Increase Productivity**
  No longer are you restricted to communicating with your workers via status messages or voice. Unified voice and data across multiple networks means you can share information with the right people, by the fastest and most reliable method.
- **Enhance Interoperability**
  With a choice of bearer always available, you can communicate dynamically with contractors and other agencies and organisations, across any network you have in common. You can even implement a secure BYOD policy for your workers.
- **Reduce Overheads**
  Without the overhead of a single, all-encompassing network across your entire coverage area, you are free to choose the quality and cost criteria for any group, situation or function.
- **Increase Coverage**
  No single technology can provide communication across the diverse terrain, variable demand and proliferating data that your organisation needs. Designed to your exact requirements, a Unified Critical Communications system minimizes coverage “black spots”.
- **Keep Workers Safe**
  Workers who understand and trust their communication networks feel safer and more confident. They know that should an accident, injury or emergency occur, they are not alone. Worker safety features, location data and alerts can operate across different networks and provide real time visibility, so you know instantly when and where help is needed.
- **Tailor Solutions To Your Needs**
  Different industries and regulations, different operating processes, different environments and the availability of different network types will all influence your choices.
- **Future-Proof Your Investments**
  What’s available today is just the beginning. The right technology choice can mean the difference between stranded investments, and communications that continue to take advantage of open standards and future developments.
- **Scale Your Solution**
  A unified approach to communication means you can keep your options open. You can start small today, then add more network bearers, new developments and applications as your organization grows, your options expand, or your requirements change.
- **Safeguard Communications Resilience**
  Loss of communication at any level can be costly – even life-threatening. Building redundancy into a typical single-bearer solution carries a high capital overhead too. A unified solution gives you multiple levels of redundancy, avoiding any single point of failure automatically.

DEVELOPING UCC SOLUTIONS FOR THE REAL WORLD

How does a company or agency successfully develop a Unified Critical Communications solution? Key partnerships between users and developers are critical; the paradigm shift from voice-oriented to data-oriented critical communications opens up new opportunities for communications developers as well as for customers.

For UCC customers, the most successful partnerships are founded on open standards, to create flexible, future-proofed solutions. Real-time analytics, AI, streaming media, and advanced mobile communications, are evolving and converging, driven by IP and new connectivity paths, to open up incredible mission critical opportunities.

Unified Critical Communications offers a wider range of partnering opportunities that safeguards business continuity while embracing change. Here are some examples:

- **Customers and developers can collaborate to create customized solutions.**
  Transport for London (TfL)has partnered with Tait, to fit London's buses with Tait Unified Vehicle UCC platform to offer customized applications to passengers.
- **Developers can add LMR capability to their cellular-based products.**
  Sonim uses Tait specialist RF knowledge to integrate LMR into their ruggedized XP8 Android mission-critical smartphone.
- **Developers can co-develop new products.**
  Tait and Mine Site Technologies (MST) developed the FUSION Voice mobile radio. Combining MST's Wi-Fi based VoIP communications expertise with Tait Unified Vehicle, FUSION can roam wherever hybrid technologies exist on a mining site, below or above ground.
- **Technology companies can extend their integration range**
  Partnership between dispatch developer Tait, Avtec, and EsChat has integrated the Tait P25 radio network, ESChat's full featured PTT over LTE via ISSI, and Avtec's Scout™ Dispatch Console via CSSI.
  Tait EnableLocation provides real-time asset and workforce location tracking, in conjunction with GPS/AVL specialists Tallysman.
- **Distributors can expand their solutions portfolio**.
  Logic Wireless customers benefit from collective development opportunities between the various communications technology companies that Logic represents.

Ultimately, the strength of Unified Critical Communications is that it massively increases options for connectivity by removing the limitations of any single bearer technology. For network operators, this not only improves system resilience, but by implementing open standard interfaces, extends the operational capabilities and future-proofs critical communications systems.