FIRSTNET
Built with AT&T

Why first responders need Mission Critical Push-To-Talk

Tracy McElvaney Q&A Interview

We sat down with Tracy, who leads the FirstNet Mission Critical Solutions team, to talk about the evolution of public safety communication systems and why mission critical solutions are important to public safety. Here's what he had to say:

Q: Why is Mission Critical push-to-talk important for public safety?

A: MCPTT is a communication system that combines group communications and advanced situational awareness. It uses a highly scalable network that is more advanced than older technologies like LMR. The most important benefit of this system is that it allows public safety officials to prioritize their communications over other types of communications. This means that even if the network is busy, mission critical communications can still get through and first responders can stay connected and use the application even on the worst possible days.

Q: How is Mission Critical Push-to-Talk different from LMR?

A: LMR is an older technology that has remained relatively unchanged for 35 years. It uses narrowband frequencies and trunking technology, which allows only a few simultaneous conversations. The lower frequencies LMR uses require fewer towers but has limited over lapping coverage. LMR only allows for voice and minimal data communication and is very expensive to integrate other technologies due to its proprietary nature.

MCPTT uses a highly scalable, more advanced network. As a result, it can support many simultaneous group conversations, with video and data capabilities as well as advanced situational awareness features. It also prioritizes mission critical communications over other forms of communication, ensuring that first responders can stay connected even in busy network conditions.

Q: How does Mission Critical Push-to-Talk improve communication among first responders during emergencies?

A: MCPTT improves first responder and public safety by enabling clear, reliable communication in critical situations. The most important aspect of MCPTT is the ability to transmit and receive intelligible audio in very loud noisy environments.

First responders often operate in high-stress, high-noise situations where clear communication can make the difference between life and death. AT&T and our partners at the FirstNet Authority have worked through the standards bodies to implement updated voice encoding technology that meets or exceeds the Analog FM standard for voice intelligibility and loud-noise environments to address this. This ensures that first responders can communicate effectively and accurately during emergencies, improving safety for them and the public.

MCPTT provides advanced situational awareness, messaging and multimedia capabilities and incorporates near real-time map drawing features for improved incident management workflow. This allows first responders to share information and collaborate more effectively, even during large-scale events.

During a natural disaster like an earthquake, different agencies respond to the emergency. They must set up staging areas and operation centers and establish a chain of command. If they are using LMR radio systems, they can only communicate verbally, which can lead to misinterpretation in high-stress and noisy environments.

MCPTT allows first responders to share images or PDF files, which provides a collective understanding they can reference later. This advanced situational awareness helps responders to collaborate more effectively and saves time.

For example, suppose a firefighter takes a photo of a collapsed building. In that case, they can share it with other responders who can quickly assess the situation and respond accordingly.

Q: What are the 3GPP standards?

A: The 3GPP is an organization that brings together people who build cellular networks. Its goal is to create a set of standards that support a consistent user experience and ensure that network equipment operates in a standardized way.

MCPTT was introduced into the 3GPP organization to create a common set of parameters for

performance and operations. This ensures that the technology performs consistently to a public safety standard. With 3GPP, the focus is on what the application does to ensure that the service operates consistently across devices and solutions. This gives public safety officials the flexibility to choose a solution while maintaining a certain quality of service.

Q: What makes Mission Critical Push-to-Talk on FirstNet different from other options?

A: FirstNet is the only network that broadcasts a public safety-specific Public Land Mobile Network (PLMN) ID. This ensures that first responders have a network with reliable communication during emergencies. FirstNet also manages the spectrum set aside just for first responders, which means they have a dedicated lane of connectivity when they need it.

By combining a standardized mission critical application with a network built specifically for public safety, FirstNet provides an even higher level of resiliency, reliability, and consistency.

Q: What Mission Critical Push-to-Talk options are available on FirstNet?

A: FirstNet offers two MCPTT solutions. The first solution is FirstNet Push-to-Talk, a simple and easy-to-use platform created based on standards and contract requirements from the First Responder Network Authority. It includes mutual aid, which means that first responders from different agencies can communicate with each other during emergencies.

The second solution is FirstNet Rapid Response. It integrates into the FirstNet platform and delivers the same mission critical services with the same performance. This technology was initially developed for businesses and enterprises but has been adapted with public safety-specific features for even better performance.

Both options offer the power of choice for public safety officials, with the assurance of consistent performance in large-scale events.

Q: What are the technical challenges of implementing Mission Critical Push-to-Talk, and how can we address those?

A: One major challenge is building trust in broadband push-to-talk, as agencies have long relied on traditional LMR radios and may be hesitant to switch.

To address this, we focus on three key questions: Can we get you connected? Can we keep you connected? And does it work while you're connected? We can get agencies connected through our extensive coverage of over 2.91 million square miles. In fact, FirstNet covers 250,000+ more square miles than the largest commercial networks available to public safety. We can also handle thousands of talkers simultaneously, enabling more people to be part of the communication ecosystem. Additionally, the technology is operable in many conditions where LMR is not, such as through Wi-Fi, cellular and in-building solutions, which can help agencies stay connected even in challenging scenarios.

Despite these advantages, some agencies may still prefer using traditional radios alongside MCPTT. In that case, we offer interoperability between the two systems, allowing radio and broadband users to communicate in the same talk group. This can ease the transition to broadband technology without disrupting current operations.

Q: What are the biggest challenges for public safety agencies when adopting new technology, especially Mission Critical Push-to-Talk?

A: Adopting new technology can be challenging for public safety agencies. Safety and training are major concerns. Using new technology in high-stress environments can only be safe with sufficient training. Financial challenges, such as budgeting for capital and operational expenses, can also be a barrier.

In addition, some LMR incumbents have a strong hold on the community due to long-term contracts, and earning trust as an alternative solution can be a challenge. Public safety officials may also have concerns about the reliability and performance of the new technology, which can impact their willingness to adopt it.

Q: What security measures are in place for Mission Critical Push-to-Talk operations?

A: Security is a top priority for MCPTT operations. We start by creating secure containers within devices to protect data and audio when the devices are idle. Additionally, the FirstNet network is highly secure to help protect sensitive information.

We have also implemented comprehensive tower-to-core encryption, adding a second layer of encryption to secure the data as it moves from point A to point B. FirstNet is the only network that has implemented this level of security, ensuring that we protect public safety officials' data.

Q: What innovations do you see on the horizon for mission critical communications?

A: Today's mission critical platform adds advanced situational awareness to traditional audible communication. Looking ahead, 5G and IoT will enable even smarter devices and systems to communicate more effectively between the devices and with humans.

For example, imagine a future where traffic cameras have sensors that alert a talk group when they spot a license plate with an associated warrant. Automating processes that have traditionally been manual can save time and money while improving operations and response times.

Q: How does FirstNet contribute to the leadership of Mission Critical Push-to-Talk technology?

A: FirstNet has been critical in the leadership of MCPTT technology. AT&T, together with the FirstNet Authority, drove development of the technology, established the standards, committed to delivering it and delivered the first platform.

FirstNet leadership – both with the FirstNet Authority and at AT&T – are working together to ensure that MCPTT technology continues to evolve and improve to meet the needs of public safety. If we were to stop its work in this area, the technology would not just stand still but regress.

As we advance, we will continue to partner with the federal government to innovate and deliver technology solutions much faster than they would have been otherwise.

Q: Are FirstNet Push-to-Talk and FirstNet Rapid Response used for two different types of devices?

A: No, you can use devices that support either platform, so the device and application choice is flexible. The main difference between the two platforms is the user interface. Agencies will choose an application they can train, support, and operate with effectively for safety reasons.

The goal is to establish trust in the coverage and technology and allow agencies to choose what works best for them.

Q: What is the final thing you would say to someone who is on the fence about making the switch to MCPTT?

A: First, I encourage them to consider the direction the world is heading with public safety and the private sector partnering to take advantage of new technology. MCPTT is the future of public safety communications, providing advanced situational awareness and reliable communication capabilities to first responders when they need it the most.

Second, they should try it out if they haven't done so because it probably operates better and connects in more places than they realize. MCPTT technology has come a long way in recent years, offering significant improvements unavailable in legacy LMR systems.

Finally, I would advise them not to be afraid of merging the two systems, as there are now cost-effective ways to do it and we can assist with managing the process. We focus on delivering fundamental communications that help public safety operate more efficiently, safely and cost-effectively.

Tracy McElvaney is Associate Director, Public Safety Assurance Management, FirstNet Mission Critical Solutions. He is an accomplished leader in the field of public safety communications, and provides expert insights on MCPTT's capabilities, advantages, technical challenges, and innovations on the horizon.