In the April 9, 2025, issue of *Urgent Communications*, APCO's Chief Technology Officer Stephen Devine poses a key question: "Does public safety care whether push-to-talk communications are delivered via LMR or LTE?" His conclusion is clear--public safety users don't care about the underlying technology. What matters most to them is simply being able to communicate reliably, whenever and wherever needed.

I, for one, agree with Mr. Divine's conclusion: as long as the message gets through, that's what is important. Having once been a First Responder, I can validate they have far more pressing concerns than the technical path their PTT signal takes, or the network carrying their radio traffic. As communications providers and system operators, we have done our job well when that signal--and the one that came before it and the one after--gets through. That's the outcome responders count on, and the one they trust with their safety.

Stephen Devine points out that hybrid or converged LMR/LTE devices will continue to evolve, becoming better at determining whether to use LMR or LTE for the PTT pathway. He also recognizes how the coverage footprint expands, and thus the overall talk in and talk out performance-- consistency within a service area--naturally improves.

The idea that LMR or LTE based PTT systems are interchangeable can only be accepted once radio users are convinced that both technologies perform consistently—every time. They must also trust that the PTT will work where it worked the last time they were there. This kind of acceptance, trust, and confidence builds gradually, through reliable operations and user experience. Rain or shine, it has to work. If it doesn't, users will quickly notice and work to classify the failure. This reminds me of my experience during a major Southern California blizzard, where several leading LTE carriers began to fail several days into the event. It quickly became apparent to responders that something was wrong, as their cell phones and commercial mobile data systems stopped working in areas where they had previously been reliable. In that situation, responders absolutely cared whether PTT traffic was carried over LMR or LTE -- because LTE was beginning to fail.

Ultimately, radio users need dependable radio coverage and reliability over time to build confidence in the system's reliability and performance.

Looking ahead, we may well be approaching an inflection point in the PTT user experience between LMR and LTE. Beyond a system redundancy boost and improving talk in and out performance within the operational footprint, what other challenges does this present, and what should our next steps be?

<u>Acquisition and Recurring Cost:</u>

No question, it's going to cost more to field a radio. The acquisition cost will likely increase since there are two complex radios built into a single package. Once that capital cost is

absorbed, there is the recurring monthly charge from the LTE carrier. Many LMR systems fund their operation with a monthly user rate for each radio to recoup their costs. Adding an LTE carrier passthrough charge on top of that enterprise rate to cover LTE network access could be a tough cost-benefit proposition. Each entity will have to evaluate the cost benefit and determine how best to position and justify this new on-going expense.

Increased Coverage Reliability and Expansion:

For radio users who frequently travel outside the LMR footprint, it is easy to appreciate how the expanded radio coverage area offered by LTE can provide significant operational benefits that support their mission. However, for the otherwise rank and file radios that don't need to leave the traditional LMR footprint, what tools, long term surveillance procedures and analysis are needed to ensure that the additional capital and recurring investments translate into improved daily coverage and dynamic LMR/LTE cross redundancy within that footprint? How can we guarantee that LTE function and footprint at a given location will consistently exist and deliver a reliable user experience? And how can LMR operators effectively collaborate with LTE network providers to address these nuances?

P25 Standard Integration:

Modern LMR systems benefit from Project 25's suite of standards, as defined by the Telecommunications Industry Association. After incorporating these standards into their designs, manufacturers submit their products to the P25 Compliance Assessment Program to ensure they fully meet the P25 standard and can operate seamlessly within the ecosystem--facilitating a standard customer experience. Rudimentary functions such as call set up and system response timing, along with advanced features like scan, private call, user ID aliasing, encryption, and console operations, must work equivalently as radio users transition between LMR and LTE networks.

How is this assurance of equivalency established, measured and maintained? How are gaps that could impact operations and user experience identified and managed?

Rescaling of the LMR System:

If it turns out that LTE can reliably deliver the same high-quality user experience as LMR—achieving equivalent uptime, responsiveness, and functional parity--over time, and ends up with the same number of "9's" for reliability, could this prompt a reevaluation of how LMR systems are scaled? If we learn that LTE proves capable of bearing the operational load while providing the gold standard LMR PTT user experience, would it parlay into cost saving opportunities that reduce the size and scope of the LMR system and potentially realize a significant ongoing operational and future acquisition cost reduction? Could this

opportunity be further scaled to reduce LMR resources in selected areas of the traditional coverage footprint where there is robust and resilient LTE infrastructure, while LMR continues to serve other areas, such as remote regions, where LMR coverage is often dominate? Are there pockets of "low hanging fruit" here, ripening for a harvest, where shifting the balance between LTE and LMR could deliver tangible benefits and savings?

Security:

For an LMR system to process and coordinate PTT calls that originate on an LTE network, some degree of cyber exposure between the two systems must be established and permitted. But what kinds of real or emerging security vulnerabilities does that introduce? Could it create an unintentional back door, or a natural point for a Man-in-the Middle exploit?

While there are certainly firewalls and authentication appliances available to help protect an LMR network, those same tools are also used on actual computer networks operated by reputable organizations around the world that still fall victim to intrusion and exploitation breaches all too often. Historically, LMR has benefited from operating very securely in a standalone, air-gapped environment. In what some might call "security through obscurity," Is it wise now to expose a core LMR processing function to a disparate and potentially more vulnerable network? Should a new, purpose-designed interface–one offering maximum security and robust threat detection and response capabilities--be developed to provide the utmost degree of security?

To conclude, the public safety community rightly has far more to focus on than whether their PTT requests are handled by LMR, LTE or a combination of the two. Their mission demands attention to immediate needs, not to sorting out the intricacies of underlying communications architecture. As such, they rely on practitioners in this field to get it right and anticipate needs, evaluate tradeoffs, and put forward sound, evidence-based recommendations and solutions.

Certainly a hybrid approach may offer a fantastic and consistent user experience. In time, it could also create opportunities to rescale LMR, potentially resulting in meaningful LMR acquisition and operational cost savings, much like P25 once promised to deliver.

But with these opportunities come real *watch outs* such as higher ongoing costs for operating LMR-enabled radios including greater demands on technical staff to monitor and validate the LTE function. And in the more advanced realm--not to be discounted—connecting a traditional LMR system to an evolving LTE network introduces real cybersecurity risks that must be skillfully evaluated, respected, and actively managed.

As public safety professionals remain rightly focused on their mission, it falls to the wireless and radio communications community to understand and anticipate their technical needs, weigh tradeoffs, and develop resilient, cost-effective, and secure solutions—fulfilling this responsibility is how we best serve those who serve others.

Tim Trager served 38 years in the Public Safety Wireless Communications field, recently retired as a Division Chief from the San Bernardino County – Innovation and Technology Department. Tim holds a B.Sc. from the University of La Verne and is experienced in all aspects of governmental technology program management, policy creation, and service delivery. Tim also contributed back to the community, serving as a Reserve Fire Fighter/EMT for nearly 20 years. Tim Trager currently serves as the Vice President for the Government Wireless Technology & Communications Association.