ALMR INSIDER

Volume 10, Issue 4 October 15, 2016

ALMR Help Desk

In Anchorage: 334-2567

Toll Free within Alaska (outside of Anchorage): 888-334-2567

E-mail: almr-helpdesk @inuitservices.com

Inside this issue:

Why FirstNet Should be Data Only

It has been four years since the First Responder Network Authority (FirstNet) began operations and many more since the industry realized a need for public-safety broadband. When first conceived, FirstNet was supposed to be a high-speed data network, which would ensure first responders had access to the same high-speed data that the public used every day on their 4G Long-Term Evolution (LTE) cellular networks.

During the past four years, the purpose of FirstNet has evolved from a mission-critical data only network to a mission-critical voice and data network. Exactly how this change took place is less important than the result of this change. We need to return FirstNet to the concept of a mission-critical data-only network and focus on getting that part right. In the meantime, we should continue to use and maintain our mission-critical voice and slow-speed data LMR systems and stop telling elected officials and budget folks that LMR will go away. Public safety's mission is too important to depend on only one network for the foreseeable future.

Complexity
LMR systems across the country, perhaps as many as 50,000, are generally hardened and work well under stress. They have been refined for more than 50 years to the point that most have two or three levels of failover codified in standards such as National Fire Protection Association (NFPA) 1221 and others. By contrast, many links, servers and gateways connected by IP technology are needed for an LTE system to work and fail-soft features are not particularly inherent in LTE systems.

Centralization
The thousands of discrete LMR systems across the country are reliable, and in many cases hardened, delivering mission-critical voice and low-speed data (identification, emergency and status messages). In a world increasingly threatened by hackers, criminals and activists, putting all of the nation's three million first responders on a single network is to invite disaster. Decentralized LMR systems, many of which are not IP based, and their layers of fail-soft provide an alternative to the IP-based FirstNet, should it be taken down locally, regionally or nationally.

Timing
The successful vendor to the FirstNet request for proposals (RFP) has a massive task ahead; the RFP has 460 work tasks identified. Imagine the amount of project coordination needed to 1) build a nationwide network for public safety, 2) train public safety to use it, 3) manage the applications that are allowed access and 4) monitor/maintain the network across as many as 56 states and territories combined.

Standards
LTE systems were designed to provide high-speed data to consumer cellular devices; they were not initially deployed to support public safety, which requires functions not commonly found in public carrier systems, such as one to many push-to-talk (PTT) group voice communications and direct mode communications, or radio to radio with no infrastructure but with sufficient transmit power to support work groups within a half-mile radius. These standards will take several years to be realized.

Radios and Coverage
LMR systems generally cover the geography needed by the public safety agencies they serve, but in-building coverage has become an increasingly important issue. Providing in-building coverage for FirstNet will be expensive, and it is not budgeted for. For some time to come, LMR systems will be better able to provide in-building coverage than FirstNet will.

FirstNet has daunting economic, technical, political and execution tasks ahead. Building such a network will take more time and funds than many have envisioned, but we need to discard the idea that LMR will go away.

(Prepared by Ms. Sherry Shafer from article by Mr. Jeff Facella, Mission Critical Communications, "P25: Advances in Interoperability and the Technology's Future.")

Will LTE Replace Traditional LMR Technologies?

The major LMR vendors are shifting their focus to LTE, but does that mean the end of innovation and support for LMR technologies? The consensus of industry experts is that the answer is "NO."

LMR is not going to be replaced by LTE any time soon and all the vendors will continue to innovate and support LMR technologies for the foreseeable future. There are many factors in favor of LMR staying relevant for a very long time and it is likely that LTE will augment, instead of replace, LMR for at least a decade or more.

The number one factor for LMR staying relevant is cost. Many LMR operators have just finished converting from analog systems to digital systems such as P25, TETRA, and DMR. P25 and TETRA have been around for over 20 years (P25 was introduced in 1989 and TETRA in 1995) and yet, many operators are just now transitioning over to a digital standard or are still running analog systems. A major reason for the slow adoption rate is cost. This will be the same for system owners considering LTE. The more likely scenario will be augmenting existing LMR voice systems with LTE for data services. In fact, in the initial roll out of FirstNet, LTE is considered to be a complementary enabler to public safety systems that will sit on top of existing LMR voice systems. In addition to the cost of new equipment and infrastructure, LTE requires much more bandwidth than narrow band LMR systems and the need for sufficient spectrum is a barrier for scalable deployments throughout the world.

Another important factor is the technical challenges installers, maintainers and operators will face. One of the reasons LTE was selected as the technology of choice for broadband communications for the public safety sector is because it is the same technology being rolled out by commercial operators, so it should be well understood and easy to install, use and maintain. However, keep in mind that LTE systems for critical communications have special features and requirements that the commercial networks don't have to worry about. The primary concern being that it needs to be much more reliable as lives are at stake. It also has to operate in conjunction with existing LMR networks which are often times in the same frequency bands. This can present challenging interference issues for system designers, installers and maintainers. Other technical challenges include RF coverage and other system considerations. LMR handsets typically transmit with three to five watts of power, whereas, an LTE handset may only be capable of transmitting with about one watt. This translates directly into longer range for LMR systems. So, for an LTE network to provide the same coverage area as an LMR network, operators will need to install many more sites spaced closer together resulting in higher equipment and maintenance costs. Because of infrastructure costs, a broadband network at 700MHz will not be able to replace LMR in many locations across the US due to RF propagation properties. Matching LTE to LMR coverage and reliability is just too cost prohibitive.

In areas where there is existing LTE infrastructure, you may question why there is a need to build a second private network when the community already has an LTE network in place. The fundamental reasons is that although commercial LTE works, it is not built to mission-critical standards of reliability. Another important consideration is that when there is a major incident, many civilians will get on the network and take up valuable network resources leaving no bandwidth for the public safety professionals. In a worst case scenario, the public may overwhelm the network and all communications will be lost. This has happened many times in large disasters. There is no way to give preemptive priority to public safety traffic, so a dedicated private network for public safety is necessary.

There are many questions and concerns by the end users about LTE that must be addressed before it is accepted. LMR systems are a known quantity and reliable voice communications is the number one requirement for any public safety system. Beyond reliability, one basic questions is how well will LTE be able to handle voice and data. These questions can only be answered with empirical evidence once actual systems are in operation.

It is very likely that it will be many years, maybe even a decade before the transition to LTE is made and it may never fully replace LMR. It may just converge into a new hybrid LTE/LMR technology.

(Prepared by Ms. Sherry Shafer from "Anritsu: The Impact of LTE on the LMR Industry," pamphlet 11410-00961, Rev A, June 2016)

System Maintenance Contract Awarded

After an extensive Request for Proposal (RFP) Best Value process conducted over several months, the ALMR Infrastructure Operations and Maintenance Services (IOMS) contract was awarded on September 15, by the State of Alaska, to Motorola Solutions, Inc. with Bering Straits Information Technology (BSIT), serving as the subcontractor. The initial contract period is for two years, with eight one-year renewal options.

Prior to the awarding of this contract, the SOA and the Department of Defense (DOD) had separate contracts in place. As a result of enabling legislation passed by Congress, the DOD will be able to contract directly with the State for IOMS.

Motorola Solutions will continue to utilize the same BSIT personnel under the new contract.

(Article by Mr. Del Smith, ALMR Operations Manager)

Tech Corner: Real-World Interference Can Affect Anyone

In a previous Insider article, now-retired Technical Advisor, Mr. Rich Leber, discussed a type of radio frequency (RF) interference known as Passive Intermodulation Interference (PIMI), also called the "Rusty Bolt Effect," which obviously can occur from an unlikely source. The following article highlights the real-world occurrence of a PIMI event and demonstrates how it can not only affect public safety radio systems, but also detrimentally impact our daily lives.

Police in Evanston, Illinois, contacted the American Radio Relay League (ARRL) Lab, after an apparent interference source began plaguing wireless vehicle key fobs, cell phones and other wireless electronics. Key fob owners found they could not open or start their vehicles remotely until their vehicles were towed at least a block away, nor were they able to call for help on their cell phones when problems occurred. The police turned to ARRL for help after striking out with the FCC, which told them it considered key fob malfunctions a problem for automakers although the interference was affecting not just key fobs, but also cell phones, which are a licensed radio service.

The 600 block of Dempster Avenue in Evanston was the area in question, which was plagued by the strange radio interference problem. "This situation is indicative of what can happen as a result of insufficient FCC enforcement, especially with regard to electrical noise and non-compliant consumer devices," ARRL Lab Specialist Mr. Mike Gruber said.

Evanston authorities worried that a serious situation could develop if someone were unable to call 9-1-1, putting public safety at risk. They also were concerned that the radio frequency interference (RFI) could be intentional and indicate some nefarious or illegal activity. Given the seriousness of this situation, Gruber contacted Central Division Director Kermit Carlson, to look into the matter.

On June 2, Mr. Carlson met with an Evanston police officer, her Sergeant, a local business owner and the local alderman, and quickly confirmed that the area in question was truly plagued with an odd RFI problem. Mr. Carlson determined that the problem prevailed along a set of eight, on-street, parallel parking spots in the downtown commercial district of the North Chicago suburb.

He employed a Radar Engineers 240A Noise Signature Receiver and ultra-high frequency (UHF) Yagi antenna to survey the affected block. Since key fobs typically operate at around 315MHz and 433MHz, he looked on both frequencies. The survey identified several noise sources in the affected block, but in particular a strong signal in the middle of the block. The interference source turned out to be a recently replaced neon sign switching-mode power supply, which was generating a substantial signal within the on-street parking area just across the sidewalk, between 8 and 40 feet from the sign.

The Ventex Technology power supply for the neon sign was found to be a strong source of radio interference in the affected neighborhood of Evanston. The problematic power supply interference also disabled Mr. Carlson's cell phone when he was within a few feet of the device. He anticipated that further investigation would show that the harmful interference could disrupt licensed radio services in close proximity. Although, the troublesome transformer was not replaced, the building owner agreed to turn off the sign should problems arise.

(Recommended by Mr. John Lynn. Prepared by Mr. Del Smith from "Amateur Radio Sleuthing Pins Down Source of Strange RF Interference," ARRL Letter, August 11, 2016)

AES Encryption Available on ALMR

Although currently only implemented by local, State and Federal law enforcement agencies operating on ALMR and the Department of Defense (DOD), Advanced Encryption Standard (AES) 256 provides the best way to protect critical information from compromise and disclosure. However, if not appropriately planned and implemented with the proper procedures and policies in place, it can also impact interoperable communications.

Because both DOD and Federal agencies operate on the ALMR System, it was implemented with AES 256. NCSWIC, SAFECOM and FPIC recommend AES 256 encryption should be the goal for all public safety agencies to ensure the greatest protection against potential compromise of sensitive information and the best chance to improve encrypted interoperability.

The Department of Homeland Security Office of Emergency Communications, in its National Emergency Communications Plan (NECP) of 2008, detailed an initiative to "... implement AES for Federal responders. A standard nationwide encryption method will diminish the interoperability challenges faced by Federal responders, who previously used different methods, and will provide guidance to local and State agencies when working with Federal agencies," and to establish "AES as the uniform standard for State, local and tribal emergency responders who decide to use encryption."

Although the NECP has since been updated, the soundness of the initiative remains valid today and extends to all public safety agencies. Simply put, encryption for the Nation's first responder communications systems assures protection of sensitive information from unauthorized use.

If your agency does not currently utilize encryption and you would like to have information about how to do so, please contact the ALMR Help Desk.

(Prepared by Mr. Del Smith from SAFECOM website at: https://www.dhs.gov/Technology)

Educating Decision-makers on LMR Issues

Public safety LMR systems provide responders with mission-critical voice communications and the best possible radio frequency coverage within a given geographical area of responsibility.

These systems are designed to meet unique mission requirements and support time-sensitive, lifesaving tasks, including rapid voice call-setup, group calling capabilities, high-quality audio and guaranteed priority access to the end-user. The infrastructure equipment, user devices and methods of deployment are hardened, allowing for prolonged operation in rigorous and harsh environments with a higher level of user familiarity, availability and accessibility.

While voice capabilities are offered through other technologies (e.g., Voice over Internet Protocol, Voice over LTE, commercial voice push-to-talk), none of these guarantee the level of reliability, expedience and control needed for the demands of mission-critical voice exchanges.

At present, there is no other more reliable choice to achieve the same level of mission-critical voice capabilities as that provided by public safety LMR systems. LMR provides a critical combination of quality, reliability and assurance of access to priority communications that public safety officials need in emergency responses.

Therefore, public safety agencies must continue to seek funding for LMR systems, equipment and enhancements in order to sustain and improve mission-critical voice communications for public safety responders. Decision-makers must consider the needs of public safety agencies and the impact of funding decisions on the ability of public safety responders to effectively communicate during day-to-day incidents, emergencies, and natural and man-made disasters. Without continued investment in LMR systems, capabilities could be compromised during response operations.

(Prepared by Mr. Del Smith from SAFECOM E-pub Feb 2016)

Help Desk In Anchorage Bowl: 334-2567

Toll Free within Alaska: 888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@inuitservices.com

Website: http://www.alaskalandmobileradio.org

ALMR site 51 at Heney Range taken on January 6th of this year.

ALMR is now on Twitter!

You can now follow our feed at @ALMR_SOA

Alaska Land Mobile Radio
Operations Management Office
5900 E. Tudor Road, Suite 121
Anchorage, AK 99507-1245