ALMR INSIDER

Volume 16, Issue 2 April 15, 2022

ALMR Help Desk

In Anchorage: 334-2567

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

E-mail: almr-helpdesk @beringstraits.com

Follow us on Twitter: @ALMR_SOA

Inside this issue:

Update on TDMA Implementation for ALMR

In the July 2020 ALMR Insider, agencies were notified that TDMA Phase 2 capability would be required on any new radios added to the system beginning January 2021. This will support the system upgrade which, among other things, adds the time division multiple access (TDMA) functionality for increased channel capacity on the system.

The upgrade will double the capacity of all existing voice channels allowing for two users to share the same frequency at any one time. This means additional talk capacity on ALMR which should reduce the amount of busies. In addition, the upgrade will allow for other features in the future, as the base requirements for some newer technologies will be fulfilled.

Last year, the GTR site repeater upgrades, which is a pre-requisite to any further updates to the ALMR system software, were mostly completed. Work will continue at the radio sites throughout this spring and summer. In September, the system software upgrade is expected to occur prior to turning up the TDMA capability which is currently scheduled to occur in December.

Although older, non-TDMA radios currently on ALMR will continue to function in the frequency division multiple access (FDMA) mode, this will diminish some of the capability the upgrade is meant to accomplish. For instance, if there are ten radios on the same talkgroup at a site, and one of those radios is an older FDMA model, the controller will dynamically assign that talkgroup the older FDMA technology. This affects the capability of the site TDMA functionality and diminishes the available capacity.

ALMR recognizes that for some agencies, it may be a significant financial commitment to replace existing radios with those capable of the newer technologies. It is our goal to allow sufficient time for budgetary and purchasing processes to take place, without being an undue burden. At the same time, the State of Alaska and Department of Defense have spent over $24 million for the upgrade and equipment refresh, and it's critical for them to get a return on their investment for that expenditure. Therefore, at its April meeting, the User Council recommended a goal date of December 1, 2026, for FDMA radios to be replaced by all member agencies.

Agencies are encouraged to immediately review their radio inventories, determine if any units require replacement, and to begin the process. They should also contact their radio dealer to determine if any new radios they may own support TDMA Phase 2 and if the feature is currently enabled. Motorola radios on the system prior to October 2020 that support TDMA will be upgraded to enable the feature at no charge to the member agency as part of the State contract with Motorola. Agencies will be contacted individually with further information on the flash upgrades.

There will be some programming steps required during the transition to TDMA, and the schedule for the upgrade is subject to change due to a number of external factors. ALMR will publish a checklist for agencies with the next steps related to the transition in the near future. If you are currently purchasing radios or having them reprogrammed, please contact the Operations Management (OMO) for guidance as some of these steps may be able to be accomplished now.

Please direct any questions regarding the TDMA upgrade to Operations Manager Mr. Dan Nelson at dan.nelson@wostmann.com or 907-777-1109. The OMO will also be holding a "town hall" discussion on the upgrades and other matters of interest on Tuesday May 3 at 10:00 a.m. via Microsoft Teams. An invitation to all agency POCs will follow by email.

(Article by Mr. Dan Nelson, ALMR Operations Manager)

International Wireless Communications Expo 2022

The International Wireless Communications Expo (IWCE) is an annual conference focused on mission critical communications. Most major communications companies have a presence, as well as experts from the public and private sector that represent statewide and local radio systems, mobile phone networks, and organizations representing engineering and standards compliance.

During the show this year, several tracks were available that focused on technical and engineering issues, land mobile radio, LTE and mobility communications, and 911/ Emergency Communications Centers. These tracks included quick power sessions, longer workshops, and case studies on real-world events.

The show, as it did last year, had a focus on the convergence of land mobile radio and mobility technologies. There are currently products that are being released that allow for some land mobile radio networks to connect to various products through the "cloud." There are certainly some real-world applications for this type of connection; however, it was obvious that the behind-the-scenes infrastructure is technically complex. The applications and usage of these integrations are different depending upon the needs of each radio system and its users. ALMR is currently a closed system, which means there are no outside connections via the internet or "cloud" and the current software release the system uses does not support such services. We will continue to evaluate the technologies becoming available after we complete the core software upgrade this year, in concert with DOD security and review requirements.

Another focus at the show was cybersecurity, and the threats that evolve daily. Due to current geopolitical tensions, it is expected that cyberattacks on the U.S. will continue to increase, and there have been some documented cases of attacks against radio systems and 911 centers. There are many resources available through the Cybersecurity and Infrastructure Security Agency (CISA) to help identify and mitigate cyberattacks, some of which are linked from the front page of the ALMR website.

Other hot topics included discussions regarding in-building wireless coverage, both talking about land mobile radio and 5G/LTE coverage. Many of these discussions revolved around current and proposed National Fire Protection Agency (NFPA) standards and the technical compliance required for building owners and radio system managers. This issue has recently come up for discussion as it relates to ALMR, and there is a group currently working to provide guidance in local areas.

As always, there was a lot of time and discussion looking ahead at the future of emergency communications, developing technologies, and how the challenges on the horizon will be met. This included basic voice functionality (still acknowledged as the core of mission-critical communications), data and telemetry from devices, integrations with dispatch equipment, processing of video and other situational awareness, and many other items. The show was a valuable forum to talk with vendors, other system managers, and other professionals in the field.

(Article by Mr. Dan Nelson, ALMR Operations Manager)

AT&T Calls for LMR-like Hardening/Coverage for FirstNet In-building Systems

AT&T supports the notion that in-building systems supporting first-responder communications on FirstNet should meet public-safety-grade requirements for coverage and resiliency. Steve Devine, AT&T's director of public-safety policy and strategy for FirstNet, said that in-building coverage requirement for FirstNet on 700 MHz Band 14 spectrum should mirror the requirements that fire codes have for land-mobile-radio (LMR) systems, which would require additional hardening of the systems and mandate coverage in areas of structures where public -safety works.

"FirstNet is public safety's network," Devine said during a session at IWCE 2022. "We really feel that the in-building solution needs to be a step up beyond what we would do commercially in those buildings. We have a model that works in conjunction with original equipment manufacturers (OEMs) and integrators to bring the signal source to that building, so the distributed antenna system (DAS) providers can work with that and work with the building owner in that space.

Meanwhile, the Safer Buildings Coalition (SBC) is in the process of developing a handbook that outlines the best practices that stakeholders can use when developing in-buildings systems designed to provide first responders with communications. The first edition of the handbook is expected to be available by the end of the year, according to SBC Executive Director Alan Perdue.

Devine said the in-building industry and public safety should not count on AT&T funding an in-building initiative. One potential alternative source of funding for an in -building FirstNet initiative is the FirstNet Authority, which has long included in-building coverage in its roadmap document and is projected to have about $15 billion to reinvest in the FirstNet system.

Jeff Johnson, a former FirstNet Authority board member, stressed that such an investment decision would be at the discretion of the board, "There is a return-on-investment value proposition to be made. It's within their power, and I think that, if you present them with a business case, I fully expect them to take it seriously."

(Excerpts taken from article by Donny Jackson, March 23, published in IWCE's Urgent Communications e-newsletter)

Managing System Changes

As technologies continue to grow and evolve, a host of new products are flooding the marketplace in the public safety communications space. We are seeing products that promote the connection of land mobile radio and LTE mobility technologies, those that aggregate data from CAD and other situational awareness tools, the latest in recording and dispatch systems, and more.

Before considering a technology solution, it's important to understand what the benefits will be for your agency, and conversely what changes to processes, existing technology, dispatch procedures, and other components of critical communications will be necessary. Often, potential new products are investigated as a fix to a previous failure or difficulty, or are seen as tools that can increase efficiency, reliability, and safety for first responders. All of these use cases are valid, but it's important to fully evaluate the root cause of past issues. Sometimes another technological tool is not the best solution, but a correction to a process, procedure, or training will provide a long-term, more sustainable fix to the issue.

If new tools or processes are seen as an appropriate next step, ensure all current stakeholders are involved before proceeding. Within your organization, will the new tools affect a current process for your responders, management, or administrative staff? We often leave out users from the process, and you are encouraged to have some end users participate in demonstrations and the request for proposal (RFP) evaluations to provide valuable input from the "boots on the ground." In addition, you may wish to include your dispatch center, IT department, records manager, and administrative staff in the process – chances are they will all be affected or have a stake in some way.

New solutions that involve the ALMR system must go through the change request process that is outlined in ALMR procedure 400-3. This includes any tools that utilize ALMR radios, transmission of voice and data over the system, or changes to the infrastructure of dispatch centers and equipment that is directly connected to the system. The process is carefully coordinated to ensure that a potential change:

- Does not adversely affect the system or other members,
- Is compatible with the existing technology and software operating on the system,
- Is compliant with Department of Defense protocols and requirements, and
- Will not pose a security risk to the system.

If you are investigating the purchase of any new equipment or solutions, please give the operations management office or help desk a call as early as possible in the process. ALMR staff can provide guidance out the outset of the process, assist with the change request process proactively, and help communicate with the vendor about any technical specifications.

(Article by Mr. Dan Nelson, ALMR Operations Manager)

Cybersecurity Best Practices for Critical Infrastructure

Because of their importance and the vital services they provide, critical infrastructures are an attractive target for cyberattacks by hackers who have a variety of goals, from making money to disrupting society. The most common cyberattack right now is ransomware which hackers use to infiltrate a system and then lock down key data/systems until they are paid a specific amount. Without proper backup, many organizations find themselves forced to pay. Energy providers are currently the most often targeted organizations by phishing attacks aimed at creating network entry points for ransomware.

The focus on critical infrastructure led the federal government to take steps to ensure entities are protecting their systems and also recently set up advisory bodies focused on combatting cyberattacks. The Department of Homeland Security (DHS) established a Cyber Safety Review Board (CSRB) aimed at improving cybersecurity, which will review and assess significant cybersecurity events in order to better protect government, critical infrastructure, and industry.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) has provided three key practices for protecting critical infrastructure against cyber threats: "be prepared, enhance your organization's cyber posture, and increase organizational vigilance."

To protect organizations of all types against cyberattacks, Chuck Brooks, a professor of cybersecurity at Georgetown University and a former U.S. Senate cybersecurity adviser, recommended a cyber plan that encompasses these three ideas. To help protect their networks, organizations across the spectrum from public safety to critical infrastructure should practice good cyber hygiene including using strong passwords and two-factor authentication and staying off public networks. These basic cyber hygiene steps help make an organization's systems harder to hack into. Another key step to ensuring strong cybersecurity for your system is constant monitoring so you can be aware of any potential threats that do manage to make it into your system.

One key consideration with any network is the human factor. No matter how strong the technology supporting an organization's cybersecurity is, that technology can be undermined by careless or undereducated employees. User agencies are reminded that ALMR is a closed system and they should track individuals with access to the system and never utilize any outside media on the system. These are the two most prevalent threats to our network at this time.

(Article by Danny Ramey; excerpts taken from Radio Resource Mission Critical Communications Spring 2022 State of the Industry)

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

National Telecommunicators Week

ALMR is proud to serve our first responders and others that help keep our communities safe. The group of people that we don't see are often referred to as the first, first responders – the telecommunicators that answer emergency calls. Dispatch responders provide information updates and play a key role in keeping our first responders and public safe.

The general public often interacts with public safety agencies first through our dispatchers, whether that be a routine question or a life-threatening emergency. Far more than just answering the call, dispatchers often have to receive training on police, fire, or emergency medical service protocols. They must gather information while keeping callers calm and cooperative, provide life-saving instructions, and relay all of that information via computer or radio. Dispatchers act as the first line of communication between people who call 911 and responding officers, paramedics, and firefighters.

The second week of April is designated as National Telecommunicators Week, a time for us to honor the dedication and skill of the voices behind the headset who help save millions of lives every day. Initially started as a local initiative in 1981 by Patricia Anderson of Contra Costa County, California, it later went on to become a nationwide, week-long event. In 1991, it was successfully proclaimed by Congress and signed by President Bill Clinton, and in 1994 it was formally and permanently recognized.

On behalf of the staff of ALMR and all of our public-safety agencies in Alaska, thank you to all of our dispatchers for your service and calm voice every day of the year.

(Article by Mr. Dan Nelson, ALMR Operations Manager)

Help Desk (In Anchorage Bowl): 334-2567

Toll Free within Alaska: 888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@beringstraits.com

Website: http://www.alaskalandmobileradio.org

Follow us on Twitter: @ALMR_SOA

Did You Know?

Radios should always be programmed to switch to one of the owning agency's monitored talkgroups when an E-Button activates. This allows for immediate identification of the radio and determination of the individual assigned to it. Agencies can also elect to execute agreements with specific dispatch centers to monitor their alarms. (ALMR Subscriber Emergency Button Activation Procedure 300-7)