ALMR INSIDER

Volume 7, Issue 1 January 15, 2013

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:

New Standards for Hazardous Location Radios Could be Final by Year End	2
iButton Support	2
Encryption 101 - Securing Your Voice Communications	3
ETS Gears Up for a Very Busy Year	4

Robust Public Safety Systems Weather Super Storm Sandy

During Super Storm Sandy, the FCC reported that at one point 25% of all cell sites in the affected area were out of service. Reportedly, the NYPD and the FDNY communications system did not have any outages during the storm with the exception of one site where the generator ran out of fuel and that was corrected within a few hours. These failures not only affected cell phones and wireless communications, they also involved land-based communications. Wired phone and cable services were disrupted and the Internet was unavailable in many areas

First, it is important to understand that unlike today's Public Safety radio systems, such as ALMR, a cell site that is not connected to the network via some type of connection - wire, fiber, or microwave - is simply a "dumb" site. Points of failure for a single cell site, excluding the network back-end systems, include connectivity failures, power failures, batteries running out of power, generators running out of fuel, tower or structure damage, damage to antennas, and damage to equipment in the shelter. That is seven possible points of failure per cell site. While the same number of failure points are also applicable to Public Safety systems, as mentioned, there are also at least three levels of communications fallback for the Public Safety voice systems, as opposed to zero for commercial cell sites.

Public Safety sites are also usually connected to their network by wires, fiber, or microwave, as is the case with ALMR. However, if the site is part one of the advanced Public Safety networks, such as ALMR, and it becomes disconnected from the network, there is a built-in fallback mode that will turn it into a standalone, but functioning site (site trunking). If the site fails for other reasons, e.g., a power outage, generator failure, or damage to the antennas, and is knocked out of service, Public Safety still has one level of fallback that is not available today over commercial wireless systems. Public Safety voice devices are designed to operate in what is called talk around, simples, or tactical mode. This means that units can talk to each other a where no radio site is up and operating. Simplex is the final fallback for Public Safety and it works. It worked during Sandy, while cell phones people carried in areas where there were no operational cell sites were completely useless. Without a cell site, cell phones are reduced to small packages of electronic components and batteries that cannot talk to anything.

With events such as this, public safety first responders recognize that robust land mobile systems, such as ALMR, are and will continue to be critical into the foreseeable future.

(Excerpts taken from "Super Storm Sandy and Connectivity," by Andrew M. Seybold, November 27, 2012)

ALMR Essential to Real Time Mission Accomplishment

On November 28, 2012, the Federal Bureau of Investigations, Alaska Medicaid Fraud Unit and other Alaska law enforcement agencies simultaneously executed three Federal search warrants in Wasilla, Anchorage and Soldotna.

Mission requirements and agent safety dictated that all members of the team, regardless of agency, be able to communicate clearly and rapidly. Dozens of Federal and State law enforcement agents utilized the ALMR system to great advantage coordinating their efforts, seamlessly passing information amongst the geographically disparate teams as well as command post executives. Throughout the operation, the ALMR System provided the clear, reliable and secure radio communications essential to a successful outcome.

(Article submitted by Darrin E. Jones, Assistant Special Agent in Charge, FBI Anchorage)

New Standards for Hazardous Location Radios Could be Final by Year End

The two different draft standards for certifying two-way radios and other equipment used in Class I, Division 1 hazardous locations are moving forward and will likely be finalized by year-end. Each standard gives two-way radio manufacturers a less stringent option of certifying hazardous location radios and accessories than a standard implemented at the beginning of the year for other hazardous location equipment.

Telecommunications Industry Association (TIA) 4950 is moving through the American National Standards Institute (ANSI) publication process following a ballot and appeal cycle that closed Oct. 14 with no appeals filed, said Brian Martens, TIA TR8.21 committee vice chair. The document was previously released as a TIA document, and it will take several weeks to complete the ANSI process.

The TIA document is relevant only for handheld, battery-powered portable radios. TIA 4950 is a reincarnation of the previous Underwriters Laboratory (UL) standard for hazardous location equipment, UL913 edition 5. Martens said the document doesn't have power limitations for portable radios, one of the main complaints from end users with the standard that went into effect Jan. 1. The recent adoption of the International Society of Automation (ISA) standard by Factory Mutual (FM) Approvals, via its 3610 document, for other hazardous location equipment would have effectively reduced the power of portable radios, affecting communications network coverage and performance.

TIA is moving to create the next draft of TIA 4950 to remove some nonessential portions. The original UL standard was written for all equipment used in hazardous locations, not just two-way radios.

A new FM Approvals standard, FM 3640, is also specific to two-way radios and has gone out for review several times this year. "We needed to address the manufacturers' questions on whether the new standard would impact the performance aspects of radios as needed by the end user community. That's always been the major concern," said Bob Martell, director of electrical standards at FM Approvals. He said the American Petroleum Institute (API) accepted the draft FM 3640, which was distributed to interested parties for review. However, the National Public Safety and Telecommunications Council (NPSTC) voted no in October on the latest FM 3640 draft, said Paul Szoc, chair of the NSPTC intrinsically safe (IS) radio committee.

"NPSTC needs clarification so the continued viability of portable radios with up to 6 watts of RF power output essential to public safety and other critical operations can be better assessed," NPSTC said in a statement. "Any reductions in the power level of portable radios that would be required to meet the FM standard would also impact the entire system design and the performance and longevity of those systems, not just the portable radios themselves."

Martell said that based on how the standard is written, there is no issue with a manufacturer designing a product with a power output that meets user needs. He said the standard identifies the radiated power, which depends on the type of antenna used. "For end users, they shouldn't see any difference as far as the radio performance," Martell said.

(Article from Radio Resource Magazine On-line, by Sandra Wendelken, Editor, November 14, 2012)

Radio iButton Support - Motorola® Units

For those of you that program your agency Motorola™ radios, and those that want to, you need to purchase a few items. The first item is a dongle (a USB or parallel port device which allows you to plug into your computer and read the iButton), and the second item is the iButton itself, which is loaded with flashes for things like firmware updates by Motorola® or the ALMR System Management Office (SMO). These two items, along with the Motorola Customer Programming Software (CPS), and a programming cable (this cable goes between your computer and the radio) will allow you to program your agency radios.

As a cautionary note, it is highly recommended that you be familiar with radio programming before tackling this project. One misplaced or mistaken key stroke can have a drastic impact on your agency's radio communications.

The SMO does not furnish or sell dongles, iButtons, CPS, or programming cables. However, they can be purchased through Motorola™ Sales/Support by calling 1-800-422-4210 during their normal (CST) business hours. For further information on iButtons, you can call the ALMR Help Desk.

NOTE: Other vendor radios use software keys, which are obtainable through the SMO.

(Article contributed by Mr. Rich Leber, ALMR Technical Advisor)

Encryption 101 - Securing Your Voice Communications

Secure Voice communications are becoming more of a necessity than a luxury on today's public safety radio systems like ALMR. Sensitive radio traffic can be vulnerable to "Scanner Land," which can jeopardize the safety and security of both the first responders and the public. Whether it's an officer trying to locate a subject, a paramedic resuscitating a patient, or a firefighter searching a building, these real-time communications should be secure from the criminal element and general public.

However, with encryption comes increased complexity, cost, and need for management. Because radio systems, manufacturer's products, and functional operations are varied, this article focuses on two general descriptions of encryption architecture: over-the-air rekeying (OTAR) and key fill device (KFD), such as ALMR key variable loaders (KVLs).

Over-the-Air Rekeying

OTAR, which is available on ALMR, is a method to load and activate cryptographic "keys" into radios remotely using data packets transmitted over the air on the radio system. This platform also requires the use of a key management facility (KMF), which consists of a computer server or network, associated software application, and cryptographic hardware. Both the Department of Defense (DOD) and the ALMR System Management Office (SMO) manage KMFs. The OTAR function allows the encryption doctrine to be centrally managed, planned, and executed, as is the case with ALMR, so the deployment of new encryption key assignments can be effectively distributed to each user group.

This method is highly desirable if there are a large number of encrypted radios, on the system, when encryption keys need to be changed frequently, or when there are multiple encryption keys and user groups. It is a logistical nightmare, especially true of Alaska, if a team of technicians has to go out and reload or "touch" every radio as there are hundreds, or thousands, of users spread out over the state.

Key Fill Device (Key Variable Loader)

The second method discussed is a scaled down version in which only a KVL is used to load an encryption key into a radio, console, interface, or base station. The concept maintains that encryption should be a secure and separate process from programming the radio. This type of deployment means that each radio needs to be "keyed" before deployment, but when it comes to time to change the encryption key someone will have to physically rekey all of the radios. This hardware platform is less expensive than OTAR and is easier to implement on a smaller scale, but you'll spend much more time planning, managing, and executing the encryption doctrine over the life of the system. This is a typical tradeoff with most technology today when technical complexity and equipment costs are higher, but operational complexity and user impacts are lower. In addition to OTAR, KVLs are used for ALMR radios in certain instances.

Encryption Algorithms

Two common types of encryption algorithms are used in today's systems. They are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES**).** ALMR uses AES encryption. DES uses a 56- or 64-bit key, and AES uses a 128- or 256-bit key, making the AES algorithm more secure. The federal government adopted the AES standard in 2002, so for encrypted interoperability with federal agencies, the AES standard is mandatory. Encryption and interoperability don't always mix; therefore, it's critical that key assignments be managed among system managers and user agencies. This adds another layer of complexity to the management of encryption but helps prevents problems that may arise.

Managing Security

No matter which method of encryption is deployed, whether it be for a trunked system or a conventional channel, encryption and security policies and procedures should always be followed. There are a number of circumstances to consider when using encryption, such as controlling your radio assets.

Below are a few functional questions and topics to consider when discussing/utilizing encryption:

- Which agencies and talkgroups/channels will have encryption?
- Will the consoles need encryption?
- Will there be multiple encryption keys and when will they change?
- Will talkgroups/channels be strapped clear or coded, or will the user have the ability to select between clear and coded communications?
- Who has access to the encryption keys, and how are radio assets controlled when they have active codes in them?
- Will the user be able to "zero" the encryption key?
- How are radios kept secure when not in use?
- If a vehicle goes in for service and it has an active key in the radio, what actions must be taken to prevent compromise of the talkgroup/channel?

As public safety communications become more sensitive and sophisticated, the need for deploying and managing encryption becomes increasingly evident. The use and management of encryption on ALMR is complex, but the benefits of confidentiality, safety, and security to ALMR first responder agencies cannot be ignored. If you have questions about encryption on ALMR, please contact the Help Desk or the Operations Management Office.

(Excerpts taken from the November 2012 Washington State APCO/NENA Chapter Newsletter)

ETS Gears Up for a Very Busy Year

The Alaska Land Mobile Radio Communications System (ALMR) is able to provide "wide area" communications as a result of the connectivity provided by the State of Alaska (SOA) Telecommunications System (SATS). A fully functioning, well maintained SATS is critical to the success of ALMR. Continued improvement and upgrades to SATS are planned for 2013.

The Enterprise Technology Services (ETS) team is currently focused on detailed project planning for the onset of spring weather and the associated rush of activity that accompanies this time of year.

In addition to their established preventative maintenance program, the ETS leadership team has approved 35 projects to commence this year. These projects are located throughout the State and address the top needs of SATS.

The projects are varied in scope, duration and implementation strategies, but all were vetted and prioritized based on common criteria.

The team began with almost 80 projects and reviewed each based on the project's contribution to the SATS system in the following areas: security, capacity, resiliency, reliability, efficiency, general system preparedness, and those that were requested by a specific customer and funded.

The list of projects was reviewed with the ALMR User Council at their December monthly meeting.

If you would like a copy of the project listing or have any questions regarding a particular project, please feel free to contact Mr. Adam Paulick or the published project owner.

ETS is looking very forward to a productive and safe 2013.

(Article submitted by Mr. Adam Paulick, State of Alaska ETS, SATS Program Manager)

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

2012 FACTOIDS

Total Voice Calls: 11,458,239 (cumulative)

Total Data Allocations: 4,253,624 (cumulative)

Agencies on ALMR: 116 (end of 2012)

Subscriber Units on ALMR: 16,408 (end of 2012)

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