ALMR INSIDER

Volume 6, Issue 1 July 15, 2012

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:

Portable Radio versus Cell Phone - Why Size Matters

It's been asked before and it will be asked again. "Why are two-way radios so big and why can't they be as small as cell phones? " While two-way radio devices allow for voice communications similar to cell phones, they are different on many levels. There is a natural tendency to compare the two because of how prevalent cell phones have become. The following differences should help users and funding bodies appreciate the utility and design of two-way radios.

Target Markets - Two-way radios are one-to-many communications devices and required tools of the trade for many professionals in industry/ government. Cell phones are one-to-one communications devices used for individual calls.

Direct Mode - A higher power output level increases reliability of a feature of two-way radios that is unavailable in cellular - direct mode operation/ repeater talk-around (conventional). This feature allows users to communicate directly with each other in case connectivity is lost with the infrastructure (tower/site). While shorter in range and limited in the number of subscribers that can communicate, having limited communications is better than none at all. Cell phones don't have direct mode because minute usage is tracked by the infrastructure for billing. Low power levels of cell phones also make it an impractical feature.

Power Amplifiers - High-power output levels impact product design because they need large high-power amplifiers (PAs). Low power output devices can use small PAs. In addition to high PAs, frequency band also impacts the size of the components inside the device. A VHF radio has longer wavelengths and components tend to be larger. High PAs also require a larger heat sink for dissipating the heat generated by the device. This drives a larger physical form and adds to the weight. With cellular, the smaller PA generates less heat, allowing for a smaller heat sink/device. Proper heat dissipation is critical for the safe use of any device.

Loudspeakers - Most two-way radios have another high-power requirement - the loudspeaker. With cell phones, users put the device directly on their ear or conference call inside an office environment. Radios are found in high-noise industrial environments or situations with a lot of background noise. Loudspeakers require higher amperage to drive the speaker element to create the appropriate audio sound pressure for the user to hear above external noise. Higher amperage requires a larger battery, impacting radio size. The size of the radio needs to be at least as wide as the speaker.

Ruggedization - Operating in rugged, highly-industrialized and possibly hazardous environments, two-way radios require much thicker housings, stronger metal frames and critical sealing from hazardous elements, resulting in increased weight. Drop your cell phone a few times and it will break. Ruggedized industrial-grade two-way radios will not break under normal conditions in industrial environments.

Encryption - Two-way radios can be equipped with government-grade encryption for voice transmissions. This requires the highest levels of security, which means adding more circuitry and hardware inside the radio. If cell phones had to meet this kind of sophisticated user requirement, they would be bigger and heavier.

User Needs - Firefighters wear specialized gear to protect themselves from heat, fire and chemicals. They can't remove their gloves to operate a radio. If the radio is too small, it is difficult to handle and easy to drop. Recently, interoperability requirements across frequency bands have driven the creation of new multiband radios containing two or three separate transceivers plus shielding between the transceivers to prevent interference. All of this inside a single housing means a larger/heavier device.

Excerpts taken from Radio Resource Magazine, Sizing Up PMR Devices by David Lum, 12 Jul 11

Configuring P25 Radios for More Reliable Security

The user interfaces of most P25 radios are highly configurable by an agency's radio technicians, through the use of "customer programming" software provided by the manufacturer. Existing P25 radios can be configured to have much more reliable security behavior, with better feedback to the user and more intuitive operation, than the default configuration provides. Encrypted radios used in tactical law enforcement operations might be considered for configuration according to the guidelines in this article.

The Motorola Astro25 radios (e.g., the XTL-5000 mobile radio and the XTS-5000 portable) were used for terminology and illustration by the writers of the article. Most other vendors' P25 radios have similar configuration capabilities, but they may use different terminology from Motorola. Contact your radio vendor for specific information on how to accomplish a particular configuration.

The behavior of the "secure" switch is a source of confusion among even trained users. Aside from its obscure labeling (a zero for clear mode and a zero with a slash for encrypted mode), it is often out of view, can change position if touched, and does not provide direct feedback tied to the objective of communicating in secure mode.

Encryption may be a permanently enabled or disabled function of the selected channel. That is, if an agency has a frequency called **Tac1** in which both encrypted and clear communication take place, radios could be configured with *two* **Tac1** channels, one with encryption always enabled and the other with encryption always disabled. The two channel names (as displayed on the radio screen) should reflect this, e.g., **Tac1 Secure** and **Tac1 Clear**.

On the Motorola Astro25 radios, the secure/clear switch can be disabled in the "Radio Configuration" menu under "switches"; set the switch's function to "blank." Channels can then be "strapped" for "clear" or "secure" mode in the "Personality" menu for the channel.

Another alternative, noted by the ALMR System Manager, is to configure radios with the clear text “beep” warning. If you have further questions regarding these features, please contact the System Management Office through the ALMR Help Desk. *Excerpts extracted from the P25 Security Mitigation Guide , University of Pennsylvania, 10 Aug 11*

ALMR Training Available During SOA FY2013

Over the past several years, the ALMR Operations Management Office (OMO) has received numerous requests for training on the ALMR system, MotoBridge® functionality and use of subscriber units via ALMR user surveys, e-mail and telephone calls.

In recognition of the obvious need for initial and recurring training for ALMR users, the OMO engaged in discussions in the fall of 2011 with the ALMR Executive Council, the ALMR User Council and ALMR Consortium partner, the State of Alaska, regarding requesting ALMR training funds in the State of Alaska FY2013 budget.

We are very pleased to report that Governor Parnell and Department of Administration Commissioner Hultberg requested ALMR training funds in the State of Alaska FY2013 budget. The Alaska Legislature recognized the importance of this critical public safety communications system to Alaska’s first responders and subsequently approved the training funds for FY2013, effective on July 1, 2012.

The training to be offered during the next 12 months will be patterned after the recently completed training managed by the Division of Homeland Security and Emergency Management under a Federal grant. This training was offered in numerous locations, both inside and outside the ALMR coverage footprint, and focused on radio communications concepts and the technology specifically available in that area.

The training approved in the FY2013 budget will specifically address the training needs of ALMR member agencies. Similar to the grant-funded training, the scheduling of this training will take into account agency shifts, days off and availability of volunteer personnel to attend training sessions.

Several agencies have already contacted the OMO upon becoming aware of the available training funds and we will be working with those agencies to meet their training needs. Additionally, through the User Council, this article and e-mails to ALMR member agency points of contact, we are requesting that other ALMR member agencies contact the OMO to discuss their training needs and the potential timing for the provision of the training.

Please contact the OMO by e-mail at sherryshafer@5starteam.net with training requests.

ALMR System Update

The ALMR Motorola ASTRO® platform is far more robust than previous generation land mobile radio (LMR) systems. LMR technology has evolved from proprietary, circuit-based architectures to standards-driven, IP-based networks providing increased performance and flexibility for first responders.

Similar to IT systems, components within ASTRO® platforms require frequent updates, due to the pace of changing technology, to enhance and improve system capabilities. The ASTRO® platform is designed to evolve as advancements occur and regular updates can extend its lifespan indefinitely. The change from the point-to-point architecture of legacy systems to IP-based networks also has implications for network security and information assurance.

Additionally, today's LMR systems involve a much higher content of third-party technology that has implications on refresh cycles (updates) for system components. To ensure optimum performance and security of the ALMR System, regular updates to anti-virus definitions for operating systems (OS) and intrusion detection sensors are critical. Pre-tested software security (PTSS) patches for the OS and application software (i.e. Microsoft, Sun, Red Hat, Oracle, VMware) are also necessary.

The ALMR System was last updated in 2006 from version 6.8 to version 7.1.1. Motorola® system software release is now at version 7.13 and Motorola® only provides version support back to five iterations. Therefore, effective July 1, Motorola® will no longer provide PTSS patches for version 7.1.1 on ALMR. To take advantage of advances in LMR technology and ensure secure operation and optimum performance, a System update to version 7.9 is necessary at this time. A subsequent exercise of the System Update Assurance II (SUA II) option will bring ALMR to system software release 7.13.

Late last year, the ALMR Executive Council requested the Department of Defense (DOD) and State of Alaska (SOA) infrastructure owners seek funding to update the ALMR System in SOA FY13. Both DOD and SOA have been successful in obtaining funding, and contracts with Motorola® were to be in place by July 1. Current planning calls for the update process to commence in August.

To maintain the current level of interoperability that exists between ALMR and the Municipality of Anchorage (MOA) 700MHz AWARN system, that system also requires updating. However, the MOA was unable to obtain the necessary funding. Pending the future ability of MOA to fund the update to AWARN, only a limited level of interoperability will now exist between the two systems through the utilization of MotoBridge® and console patches.

Dispatch Incident Command Systems

ALMR Incident communications are facilitated through the development and use of a common communications plans and interoperable communications processes and architectures, which are generally dispatch centric.

A critical incident, whether caused by acts of nature (geological/weather caused disasters), acts of man (terrorism, crime), or acts of happenstance (vehicle accidents, freak accidents), must be handled proficiently and effectively by the agency responsible for handling it. That agency's dispatch center must be able to support the field response in a proficient and proactive manner.

The Communications Center has a critical responsibility to the community, and to its own responders, in managing the incident effectively. An agency's standard operating procedures, protocols, plans, and procedures form the basis for dispatch operations, especially during the less frequent, high-risk major incidents.

When an extraordinary incident hits a community, the dispatch center is thrown into an exceptionally busy period of critical, peak activity. There is the potential for chaos to reign, or for conflicting orders from multiple supervisors to throw dispatch operations into disarray. Having a standardized method of managing extraordinary incidents in the dispatch center will maintain a smooth operation and maximize support to the field responders. A manner of incident command, modeled after the field Incident Command System (ICS) system, geared for the needs and responsibilities of fire, EMS, or police dispatch, has been found useful in establishing a standardized, modular, and flexible means of managing dispatch responsibilities during extraordinary incidents.

Neither dispatch centers nor responding agencies can effectively plan for *every* potential emergency eventuality. We can only prepare for *most* eventualities by having a standard methodology for managing most kinds of critical incidents. That methodology can then be adapted to virtually any type, kind, or severity of incident.

The Key is *Standardization* - of command, of accountability, of resource management, of incident organization, and of tactical planning within the dispatch center. All of this equates to what already exists within ICS. By transforming Field ICS into *Dispatch ICS*, critical incidents can be managed in the dispatch center using the same function-based method as field ICS.

Dispatch ICS gives supervisors a starting place to begin a standardized method of managing the dispatch center during extraordinary events without having those events quickly run out of control due to anyone's confusion of responsibilities. It also provides specific assignments to late-arriving personnel who come in to assist, rather than having them just try to find tasks to help with without specific direction (the dispatch equivalent to "free-lancing" on the fire line).

Excerpts taken from 9-1-1 Magazine, Dispatch ICS by Randall D. Larson, 8 Aug 11

State Feasibility Study Supports ALMR

The approved State of Alaska FY2012 operating budget contained legislative intent language directing the Department of Administration (DOA) to provide a report to the Legislature in January 2012 addressing the viability of the Alaska Land Mobile Radio (ALMR) System. In response to the Legislative request, DOA contracted with an independent third party, World Wide Technology, Inc. (WWT) to conduct the feasibility study to determine whether continuing to participate in ALMR was in the States interest.

Additionally, the study was to provide an assessment of the impact to the ALMR partnership from the transfer of ownership (divestiture) of United States Army-Alaska (USARAK) radio frequency (RF) equipment at 41 state-owned communications sites over to the State.

The following is an excerpt from the Executive Summary of the study:

> "ALMR is a very effective system that greatly enhances wide area interoperable communications. Many of its current shortcomings are due to insufficient user training and lack of coordination between stakeholders. There is even greater potential for ALMR once all users become familiar with the system's capabilities. Strengths and weaknesses of the system, as well as the need for additional ALMR training have been addressed in the 2010 Business Case Update and ALMR Strategic and Operational Plan (2011)"

The entire report can be viewed at: www.alaskalandmobileradio.org/documents.htm

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

FACTOIDS

Agencies: 113

Subscriber Units: 16,056

Voice Calls: 1,076,436

System Usage: 1545:06:31 Hours

Totals for June 2012

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