ALMR INSIDER

Volume 17, Issue 4 October 15, 2023

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:

NFPA 1225/IFC2021 Emergency Responder Communications

The minimum acceptable speech intelligibility of land mobile radios is influenced by a number of factors in large commercial buildings. These factors include the method of modulation, transmission bandwidth, channel spacing, received signal strength, and the ability of a radio to capture a desired signal in the presence of interfering signals, noise, and building materials. When the minimum radio signal is unable to be met in a commercial building, an Emergency Responder Communications Enhancement System (ERCES) may need to be installed.

What is an ERCES? These systems are referred to as a bi-directional amplifier (BDA) or a distributed antenna system (DAS).

A DAS is a group of antennas placed throughout a structure to boost signal coverage. A BDA extends two-way radio coverage into difficult-to-reach areas, such as stairwells, underground hallways, tunnels, parking garages, and other challenging zones. These systems greatly enhance a first responders ability to operate in a building compared to the use of the old firefighter phones, which were rarely used by law enforcement or other first responders.

In Alaska, under the State Fire Marshal's office, the regulation which quantifies the requirements for a BDA or DAS system in new buildings is 13AAC 50.025 (International Fire Code). This regulation adopts the requirements in the International Fire Code 2021 edition, specifically Chapter 5, Section 510 Emergency Responder Communication Coverage and NFPA 1225, Standard for Emergency Services Communications, formerly NFPA 1221, Standard for the Installation, Maintenance, and use of Emergency Services Communications Systems.

Under IFC 2021 Section 510, approved in-building, two-way emergency communications coverage for first responders shall be provided in all new buildings. The radio coverage within the building shall be based on the existing coverage levels measured at the exterior of the building.

A building is considered to have acceptable radio coverage when the signal strength measures 95 percent coverage in all areas and 99 percent of designated critical areas by the local fire code official on each floor of the building. This can be accomplished by requesting a site survey by an individual who is licensed by the FCC or by installing a BDA or DAS system approved by the local fire official and NFPA 1225.

There are two key safety requirements for all ERCES equipment. The first is they shall have a dedicated standby power system that will provide 100 percent system capacity for not less than 12 hours in case of power failure to the building. The second is the system shall be monitored by a listed fire alarm control unit, or where approved by the local fire code official, shall sound an audible signal at an attended on-site location and shall cover a multitude of system failures which can be located in Section 510.4.2.5 of IFC 2021.

First responders' safety while operating in commercial buildings is of the utmost importance and can be enhanced by installing a BDA or DAS system. Examples of where these systems can be installed are jails, courthouses, hospitals, factories, airports, schools, tunnels, sport venues, and defense facilities.

To learn more about the requirements for a BDA or DAS system in a building and how it can be used for improved radio coverage and enhance radio communications, contact your local fire and life safety office or the State Fire Marshal's office.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager with excerpts taken from the NFPA 1225 and IFC 2021, Chapter 5.)

New Law Makes Interfering with Emergency Communications a Crime

In 2013, a citizen repeatedly called 9-1-1 in the MatSu Valley to report the same theft, after the fact, in an effort to solicit a police response to his house. The citizen called 9-1-1 over 45 times in 3 hours intending to tie up the emergency communications lines, as well as annoy public safety responders and illicit a response to come to his house.

Throughout this process, it was found that the only criminal recourse would be the possibility of pursuing a harassment charge under Alaska Statute. In communicating with PSAPs across the State, it was discovered this was not a localized issue, and in fact, arrests had been made from the Southeast through Fairbanks over the course of a number of years and although not frequent, it occurred three to four times per year, which was enough that it needed to be addressed.

With much education and lobbying, along with a substantial increase in maliciously tying up emergency communications lines through spoofed calls, SWATT calls, other methods of prank calling, and cyber attack style robocalls intended to tie up emergency communications lines across the country, a bill was sponsored in 2021. Unfortunately, time ran out before it could be addressed during the legislative session.

The bill was reintroduced this year, and received almost unanimous support. On July 21, Senate Bill (SB) 38, "Interference with Emergency Communications" was signed into law and establishes the crime of interference with emergency communications.

The bi-partisan bill establishes that a person commits a crime of interference with emergency communication when they:
(1) Call 9-1-1 to elicit a first responder response for a previously reported incident when there has been no change in circumstances, and they have been instructed to stop calling,
(2) Make repeated 9-1-1 calls when there is no emergency, or
(3) Threaten a 9-1-1 operator during a call to 9-1-1.

Anyone who threatens a 9-1-1 operator could be charged with a Class B misdemeanor, a crime punishable by up to 90 days in jail and a fine of $2,000.

(Article prepared by Ms. Sherry Shafer, ALMR Operations Management Office, with excerpts from SB38 and historical information provided by Mr. Jacob Butcher, MATCOM.)

How critical is the DPS SATS Microwave Network?

Most users of the Alaska Land Mobile Radio (ALMR) system are unaware that the system relies upon a vast network of state-owned microwave radio sites. This microwave network connects each ALMR radio site and will allow, for example, an Alaska State Trooper dispatcher in Fairbanks to communicate with a trooper in the southeast in Ketchikan.

The Department of Public Safety (DPS) Alaska Pubic Safety Communication Services (APSCS) maintains the State of Alaska Telecommunications Service (SATS) microwave network and regularly deploys its technicians to repair or replace critical components, such as ten-foot microwave dish antennas and feedlines that occasionally get damaged by Alaska's harsh elements. In addition, the technicians must update critical software at each site on an annual basis.

The APSCS and ALMR technicians live an adventurous and sometimes dangerous life while on the job. Most of them travel year round to remote mountain top SATS sites using helicopters, ATVs, snow machines, as well as regularly climbing up to 300-foot communications towers to maintain this critical infrastructure. This physically demanding and sometimes thankless job is not for the faint of heart.

The APSCS and ALMR staffs consist of ex-military, retired law enforcement, current military members, and civilians who regularly exhibit selfless service to help keep Alaska's public-safety communications up and running at all times to support our first responders and the citizens they protect and serve.

Bottom line, without the SATS microwave network, ALMR would not exist.

(Article written by Mr. Patrick Thornton, APSCS Communications Engineering Associate 2.)

ALMR Authority to Operate

The Authority to Operate (ATO) for ALMR has been renewed until August 2026 by the Designated Approval Authority.

The focus of the Information Systems Security Manager (ISSM) during this phase is on the maintenance of the system while ensuring updates and system changes are approved prior to implementation and completed properly. Additionally, all security controls that govern the network will be tested and reviewed at a rate of one third of the controls each year until the system is submitted for the next ATO.

I would like to thank everyone for their assistance and understanding of the process that is involved in this achievement. While it does make the acquisition of incorporating new technologies into the network time consuming, it also helps to ensure that the addition of these functions does not represent a decline in the current services provided.

(Article prepared by Mr. David Reed, ALMR ISSM.)

Land Mobile Radio (LMR) for Information Technology (IT) Professionals

Information Technology (IT) professionals are often tasked with planning, provisioning, implementing and managing land mobile radio (LMR) networks with the assumption that all computer networks have the same general requirements. However, in some cases this assumption has resulted in LMR networks being inadequately provisioned, resourced, managed, or maintained. While each system is a network, significant differences between the two must be considered to address the infrastructure, planning, and lifecycle needs of typical IT networks versus the unique requirements of LMR networks. Budgets, both capital and operations and maintenance (O&M), for LMR systems are often inadequately funded due to an incomplete understanding of what is required to develop and maintain an LMR system and its supporting networks.

CISA, SAFECOM, and the National Council of Statewide Interoperability Coordinators (NCSWIC) developed the "LMR for IT Professionals" document to explore how public safety organizations implement LMR technologies, provide LMR system implementation and integration best practices, address some LMR O&M considerations, and discuss possible disconnects between IT professionals and LMR engineers regarding the key difference between the networks which include physical infrastructure spanning far beyond the building in which the system is located and may provide services far beyond the system owner's jurisdictional boundaries to entities outside of the system owner's organization.

The "LMR for IT Professionals" document:

- Introduces what LMR is and how it integrates with traditional IT systems,
- Provides a high-level overview of LMR technologies, use, and capabilities,
- Highlights how public safety agencies implement LMR technologies,
- Discusses possible disconnects between IT professionals and LMR engineers, and
- Explores best practices for planning, integrating, and implementing LMR and IT network technologies.

(Article excerpts from "SAFECOM and NCSWIC Develop Land Mobile Radio for Information Technology Professionals," Ted Lawson, March 17, 2023, and "LMR for IT Professionals," https://www.cisa.gov/sites/default/files/2023-03/22_1220_s-n_tech-policy_lmr-for-it-professionals_508c.pdf)

QakBot Malware

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint cybersecurity advisory to provide guidance to critical infrastructure for QakBot-related activity in August 2023.

QakBot, also known as Qbot, Quackbot, Pinkslipbot, and TA570, is responsible for thousands of malware infections globally. QakBot has been the precursor to a significant amount of computer intrusions, to include ransomware and the compromise of user accounts within the financial sector.

QakBot was originally used as a banking trojan to steal banking credentials and was delivered via a phishing campaign with malicious attachments or links. QakBot has grown to deploy various types of malware, trojans, and ransomware that target multiple government services to include emergency services, specifically emergency communication centers (ECCs).

ECCs should practice the following mitigation recommendations from CISA and the FBI. Implement a recovery plan to maintain multiple copies of sensitive or proprietary data, require all accounts to comply with the National Institute of Standards and Technology (NIST) standards when developing and managing password policies and use phishing-resistant multi-factor authentication (MFA) for remote access and access to any sensitive data repositories.

ECCs are encouraged to implement mitigation strategies, validate security controls, and report any suspected activities to the FBI and CISA.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the Joint Cybersecurity Advisory prepared by CISA and the FBI, August 30, 2023)

ALMR System Clearing and Sanitization

The Alaska Land Mobile Radio (ALMR) Communications System has established the necessary controls to ensure documents, equipment, and machine-readable media are properly cleared, sanitized, and decommissioned, when appropriate. Failure to follow procedures will put ALMR at risk of unauthorized disclosure of proprietary or sensitive information, legal issues, and potential Denial of Authority to Operate (DATO) under the Risk Management Framework (RMF) for DoD Information Technology (IT).

Equipment and machine-readable media assets, which contain information, or utilize memory of any type, must be cleared and sanitized by the equipment owner. Clearing is the process of eradicating data before retiring, decommissioning, or reusing the equipment/media. This includes internal memory, video memory, caches, recovery partitions, buffers, or other forms of reusable memory.

This process ensures that unauthorized access to previously stored information is denied or that the information is no longer readable by any known method.

For more information, see Information Systems Clearing and Sanitization Policy and Procedure 200-4.

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

Unlicensed Use of the 6 GHz Band and SATS

The majority of public safety microwave systems, to include the State of Alaska Telecommunications System (SATS), have licenses from the Federal Communications Commission (FCC) to use their devices in the 6 GHz band.

In September 2023, the Association of Public-Safety Communications Officials (APCO) along with several other groups, filed a petition to protect fixed operations from harmful interference from the unlicensed use of the 6 GHz band.

The FCC rules look to permit "low power" unlicensed devices to operate in the 6 GHz band so long as they remain indoors, because outdoors without walls to block the signal, these devices pose a significant greater threat of interference to 6 GHz licensees such as public-safety microwave operators.

The FCC will now accept applications of temporary fixed stations operating in the 6 GHz band. This was necessary to protect systems from interference from new unlicensed devices.

The FCC rules support the indoor-only restriction which still allows Wi-Fi coverage using indoor access points (IAPs) in the 6 GHz band for indoor-only sports venues.

SATS includes much of the physical infrastructure required for ALMR to operate and is a highly secure, multi-protocol, wide area network that is built using public-safety grade equipment and primarily uses microwave connections at 6 GHz to connect tower sites and other facilities. This is the main reason APSCS and ALMR, as the mangers for the system, strive to maintain the integrity of the system and stay up-to-date on FCC licensing and issues.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager with excerpts taken from PSC News, September 14, 2023)

Help Desk (In the Anchorage Bowl): 907-334-2567

Toll Free within Alaska: (outside Anchorage) 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?

In the event of a system disaster, the System Management Office (SMO) shall convene a System Recovery Team to create, implement, and manage an appropriate system recovery plan to enable partial resumption of mission- or business-essential functions within five days of activation. The plan shall be tested annually, and all results shall be recorded and presented to the User Council. (System Recovery Policy and Procedure 400-1)