ALMR INSIDER

Volume 10, Issue 1 January 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:

New Intrinsically Safe (IS) Radio Battery Standard

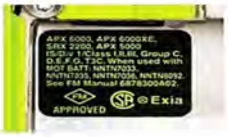
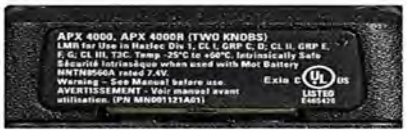
This is a follow-up to a previous article in the Insider on Intrinsically Safe (IS) radios/ batteries. Starting January 1, 2016, Motorola Solutions® radios will be accredited with the TIA-4950 standard for Hazardous Location (HAZLOC) certification of two-way radios by Underwriters Laboratories (UL) and will no longer produce Intrinsically Safe (IS) two-way radios approved to the Factory Mutual (FM) standard FM3610_88, which expired in 2012.

As you ,and your radio fleet, move into the new year with the new standard, keep these five things in mind to ensure a smooth transition:

- FM radios will stay intrinsically safe. FM approved radios that are deployed in the field will maintain their FM IS approval status, provided that any service and repairs are done at an FM audited repair facility. All Motorola radios shipped after January 1, 2016, will be UL certified. FM approved aftermarket batteries will continue to be available for fielded units.
- FM and UL approve the radio and battery together as a system. The FM approved battery may only be used on an FM approved radio, and the UL approved battery may only be used on a UL approved radio, otherwise the certification is not valid. However, you can operate with both FM and UL approved radios in your fleet.
- Don't Mix-And-Match. Non-IS portable radios batteries CANNOT, and should not, be used with IS-labeled radio units. Doing so does not make the whole unit IS. Conversely, using IS batteries with a non-IS radio unit does not make the whole unit IS. This also CANNOT, and should not, be done.
- New UL batteries will be marked and become available throughout 2016. ASTRO 25 APX UL batteries are currently available for the APX 4000 series, and availability of batteries for the other APX radios will be staggered throughout the first half of 2016.
- Classification matters. Know the Division, Class and Group of your unit rather than simply "FM Approved" or "Intrinsically Safe." HAZLOCs can be found in many industries, including refineries, fuel storage facilities, chemical plants, grain elevators and plastics processing plants. Motorola Solutions® does not determine the need for HAZLOC products, nor evaluates the environment. The need for HAZLOC products, and the classification of the specific environment, is determined by various jurisdictional authorities such as fire marshals, insurance providers, facility safety experts, etc. Check with your local authority to confirm the HAZLOC requirements for your fleet.

Editors note: If you own non-Motorola® radios, check with your vendor regarding the use of IS radio batteries.

(Article by Mr. Rich Leber, Technical Advisor, with excerpts/content taken from Motorola Solutions® Mission Critical Mobility Business Development Group blog)

	TODAY	FUTURE
Certification Lab	FM Approvals (FM)	Underwriters Laboratories (UL)
Standard Applied	FM 3610_88	TIA-4950
Classification Rating	Division 1 Class I, Groups C, D, Class II, Groups E, F, G, Class III, T3C	Division 1 Class I, Groups C, D, Class II, Groups E, F, G, Class III, T3C
For use in Hazardous Locations	Yes	Yes
ASTRO 25 Radio Label example	 APX 6000, APX 6000XE, SRX 2200, APX 5000 IS/Div 1/Class I,II,III, Group C, D,E,F,G, T3C. When used with MOT BATT: NNTN7033, NNTN7035, NNTN7036, NNTN8092. See FM Manual 6878300A02. FM APPROVED SP Exia	 APX 4000, APX 4000R (TWO KNOBS) LMR for Use in Hazloc Div 1, CL I, GRP C, D; CL II, GRP E, F, G; CL III, T3C. Temp -25°C to +60°C. Intrinsically Safe Sécurité Intrinsèque when used with Mot Battery NNTN8560A rated 7.4V. Warning – See Manual before use. AVERTISSEMENT - Voir manuel avant utilisation. (PN MN001121A01) Exia c UL us LISTED E465426

Electronic Noise is drowning out the Internet of Things

In my continuing series on RF interference and noise, I read the following article and thought it might be informative for ALMR partnership members.

You probably have experienced electronic noise when listening to your FM radio, while traveling in your car, and you passed an electrical transformer mounted on a utility pole and the radio blared static, or if you were in Chicago on your cell phone near the elevated train when it passed and your call was dropped. This also can happen around your home from things like your electric tooth brush interrupting the TV picture and audio.

Radio-frequency noise pollution is everywhere. It will only get worse as we continue to automate our lives. You can't see, hear, taste or smell this noise. Nor can you summon it and study it at your leisure, because it comes and goes with the movement of its source and its victims.

Start with the fact that any significant digital appliance has a high-speed clock and a digital buss, and both leak radiation profusely. Electric motors and generators create radio frequency (RF) noise with every small spark that jumps between their brushes and spinning commutators. Automobile engines sputter when spark plugs fire. Computers snap and pop during the sharp transitions between ones and zeros. The high-voltage ballasts of neon signs and fluorescent lights blare a broad mix of frequencies. Industrial machines, welders, elevators, relays, switching power supplies, light dimmer switches and a myriad of other items all add to RF noise. Natural sources of RF noise also exist such as lightning and solar flares.

The problem of RF pollution falls into four categories. First, it increases the cost of deploying new wireless systems, while it reduces the battery life of handsets. Second, it creates various levels of interference across a range of frequencies. Third, interference does not – but should – figure into policies on how best to share spectrum, given that the more interference you have, the more spectrum you'll need to transfer a given amount of information. So in practice, wireless channels do not always achieve the data rates they were designed to achieve. And fourth, it is expensive to trace RF pollution to a source, and when you do, it is often challenging to get the offenders to stop offending.

The coming of the Internet of Things is going to create additional issues. It will do so by adding complex RF control chips to countless common devices, like door locks, light switches, appliances of every type, our cars, and maybe even our bodies (pace makers/ defibrillators), which will enable them to connect to the internet. Each of these chips is a potential source of noise. Plenty of technological fixes are available, of course, but the huge number of chips means that manufacturers will be more reluctant to add costly shielding, and other noise muffling features to their products. Silence is golden, but it costs more to achieve it.

However, it can get better. Today every car has a radio and the noisy spark plug problem is gone. The quieting process has continued. In the 1960s, quiet alternators began replacing noisy generators, and electronic ignitions started replacing noisy distributors. In the meantime, electronic switches were replacing noisy relays. Electric drive cars, which would otherwise produce much more interference than standard cars, are sufficiently noise suppressed for cell phone and car radios to work. That same improvement came to the workplace and home. Early light dimmer switches were often electronically noisy; today most are much quieter. Personal computers, too, were redesigned for silence, if only for the sake of their own internal and external wireless data connections.

Nevertheless, the RF noise problem is increasing. Although most devices pollute less than their predecessors, we have far more of those devices. Other sources, such as the power grid, are expanding as wind farms and solar households connect to it. Such devices need to switch large amounts of DC power at a 60Hz, or an even faster rate, whenever they feed excess generated power back to the grid. If not done properly, this could feed large amounts of noise into the power grid. This risk is magnified when solar and wind systems, which operate inside millions of ordinary homes, do so without expert maintenance.

At the same time, today's machines are more sensitive to noise than ever before. Many new wireless systems, including smartphones, are designed to operate with the lowest possible power, while still providing their intended function. This means that just a little more noise interference can decrease the coverage area.

Unwanted transmissions can be inherent in the design of the device, such as a microwave oven, whose RF cooking energy also contains a large amount of RF noise. Imperfect RF shielding can allow this energy to leak out and cause interference to other RF devices. Noise can also result from a partial failure in a device – like a tiny break in the ground shield around an insulator in the high-voltage power transmission system. Such a mishap creates an inadvertent transmitter, broadcasting at unpredictable frequencies, in unknown locations and at unexpected times.

(Article by Mr. Rich Leber, ALMR Technical Advisor with excerpts taken from an 18 August, 2015 paper written by Mr. Mark McHenry, Mr. Dennis Roberson and Mr. Robert Matheson)

Can You Use Your ALMR Radio In Canada?

Law enforcement, fire and EMS units in the United States must be able to communicate with each other and with other public safety agencies responding to the scene, including first responders from Canada, and it doesn't stop at the border.

A treaty between the U.S. and Canada signed in 1951, and ratified in 1952, allows public safety agencies to operate their mobile radios as they approach the border and to continue using their mobile radio after they have crossed into the other country. This treaty did not specifically authorize the use of portable radios and was also silent on the need for data devices – neither of which technologies existed at the time.

On October 8, 2014, the U.S. Federal Communications Commission (FCC) and Industry Canada (IC) signed a letter of intent, which clarifies the implementation of the treaty. Both countries have acknowledged that public safety agencies may also use portable radios at the border and across the border in the other country.

This Cross Border Outreach document created by the National Public Safety Telecommunications Council (NPSTC) and the Canadian Interoperability Technology Interest Group (CITIG) explains exactly what the treaty allows in simple, concrete terms and also provides website addresses for further information.

The FCC and IC have also reaffirmed their joint decision to not require the issuance of a Federal permit, or other authorization, to a public safety radio user who needs to use their licensed frequency across the border. This permitting process was provided for in the 1952 treaty at the discretion of either country and has never been implemented.

Section 90.421 of FCC rules allows U.S. public safety agencies to grant permission for Canadian first responder units to access their radio systems. State and local public safety agencies in the U.S. who allow Canadian public safety units onto their radio channels should document their approval for such access.

Article by Mr. Rich Leber, ALMR Technical Advisor. Excerpts taken from a November 10, 2015, NPSTC press release.)

Protecting Your Transmissions with Encryption

Using a public safety digital radio system does not protect your transmissions. Radio transmissions travel through the open air and are therefore able to be intercepted. There are multiple avenues for individuals to obtain services – often for free – which enable them to listen to police, fire, EMTs, etc., via a digital scanner.

Depending on the amount of money invested, individuals can listen to anywhere from 100 – 1000 different channels. There is one particular service that allows the scanning individual to simply scroll down to the desired state, and select the city or the department they want to listen in on, and there are the frequencies. The scanners are clear as day, without any interruption and static. Some sites also provide the codes police officers use to talk with one another (aka 10 codes), so the scanning individual will know what they are talking about.

So how do you protect your transmissions? You encrypt them.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but it denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, which generates cipher text that can only be read if decrypted utilizing a specific key designed for that particular message.

On the ALMR System, the System Management Office (SMO) is the primary System Key holder and is responsible for managing all System Key technology.

In order for an agency to encrypt their talkgroups, first of all the radios have to be equipped with an encryption module enabling encryption. The agency must then acquire/purchase the proper programming software, hardware (iButton and iButton readers, or equivalent security device), and licenses necessary to program the subscribers they utilize, or they must hire an appropriate vendor to do the encryption for them.

Some agencies have opted to not purchase the encryption option up front when ordering new equipment and find out later that they can't encrypt unless they either retrofit their current equipment or purchase new equipment. In either case it is an added expense that many agencies can't afford, after the fact. ALMR personnel have seen this situation several times now.

Additional information regarding encryption can be found in the ALMR System Key Usage Procedure 400-16, or by contacting the SMO Help Desk.

(Article by Ms. Sherry Shafer, Documentation Specialist, and Mr. Rich Leber, Technical Advisor. Some information derived from EFF Surveillance Self-Defense Project. "What is Encryption?" dated Nov 3, 2014 and Foundations of Cryptography: Volume 2, Cambridge university press, 2004)

Interoperability Successfully Demonstrated

Alaska Land Mobile Radio (ALMR) and Anchorage Wide Area Radio Network (AWARN) were designed and implemented to provide inter- and intra-agency interoperability for their public safety first responders. The need for this critical communications capability was shown again in November 2015.

In the early morning hours of November 14, two people were shot and critically wounded near downtown Anchorage. Initial information developed by the Anchorage Police Department (APD) indicated the suspect had fled to the Wasilla area.

The information regarding the suspect's vehicle was provided to the Alaska State Troopers (AST), who were able to locate the vehicle. Shortly after the vehicle was located, the suspect departed the Wasilla area and headed back to Anchorage with AST units following at a distance. APD Dispatch patched the AST ALMR and APD AWARN talk groups together, which allowed AST units following the suspect vehicle to talk directly with APD units in Eagle River and in the Mountain View neighborhood.

The suspect became aware of the patrol units and a high speed pursuit ensued. Subsequently, the suspect abandoned his vehicle in a heavily wooded area near Mountain View that borders on Joint Base Elmendorf-Richardson (JBER).

During the search of the wooded area, APD Dispatch added the Anchorage Fire Department (AFD) Paramedics, the JBER Security Forces, the AST helicopter and the FBI agents who were airborne in a fixed wing aircraft to the incident talk group, ensuring all responders had situational awareness. This ultimately led to the successful capture of the suspect.

The interoperability afforded by ALMR and AWARN was a critical factor in the successful and safe conclusion of this event.

(Article written by Mr. Del Smith, ALMR Operations 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

2015 ALMR Factoids

Annual Total Voice Calls:

13,879,613

Annual Total Data Allocations:

4,407,459

Total Subscriber Units*:

20,344

Total Member Agencies*:

123

(*end of year)

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

ALASKA
MUNICIPAL
LEAGUE