Steve's Scanner Shop By Steve Donnell

EXCLUSIVE: How To Decode ASTRO Digital Signals!

For the past several years now, digitally encoded(RE:NOT the same as digitally encrypted) voice signals that are being incorporated in some of the next generation of Public Safety radio systems. Here in New Hampshire for instance, the State Police have been using Astro radios since early in 1994.

SDONNELL@ULTRANET.COM

For the past 23 years now, almost all of their primary dispatch/mobile radio traffic has been in digital mode, leaving anyone with a scanner, including nearly all local Police Departments, completely locked out from being able to listen in. And as many readers know, this is an ever widening problem, as other States and cities move to new radio systems.

Recently as part of a consulting project that we did, I had the opportunity to actually "play" with a pair of Motorola's latest portable radios: The XTS3000, and their associated programming software. Within a short period of time we managed to learn quite a bit about the performance of the radios in general along with some of the key parameters about how the radios can be programmed for either analog or digital modes. In simple radio to radio transmit and receive tests, I can at least say that I was quite pleased with the quality of the receiver audio in either analog or digital modes. One aspect that surprised me was the amount of propagation delay in the receive audio. In the digital mode, this was about 200 milliseconds, and about half that for analog mode reception.

In studying the technical manual for the XTS3000, the primary reason behind this delay is simple: Receive audio demodulation, either analog or digital, takes place in a special DSP(Digital Signal Processor) circuit. In fact the XTS's receiver has no conventional FM "discriminator" detector; It's "lower" IF signal of about 450 KHz, is fed directly into the DSP where the voice audio and any "embedded" digital control signals are recovered. The time delay is simply a result of the processing time the DSP needs in order to do it's job. The longer time needed to decode the digital mode signals is due to the use of more complex algorithms(program routines) needed for such things as data error correction.

One aspect of the XTS's performance that I noticed and was a bit concerned with was in how it handled reception of weak signals. In checking the receive sensitivity, in just analog mode, we saw that as the signal level was decreased well below the receiver's "12 Db SINAD" point, there was a point where the audio being heard would simply drop out, as the DSP became unable to recover a usable signal from the noise. But somewhat more interesting, was that as the RF signal level was again increased, there was about a 6 Db hysteresis from the point where the signal had originally dropped out to where the DSP would again "lock on" to the signal and start recovering an audio signal.

In all fairness however, remember this test was done with an analog signal being fed into the radio. I can't say that with the radio in digital mode, the same thing would occur. Also, I did notice in exploring the programming software, that there is a particular parameter that can be set(albeit I believe it only applies to digital mode operation), which can make the receiver more or less tolerant under weak signal conditions. However, this type of characteristic is but one of the subtle "glitches" that can pop up with any new technology. This may also partly explain some of the troubles that have been reported in use of new digital radio systems.

The software that is used to program Motorola radios is a subject often clouded in mystery, due in no small part to the tight restrictions(and price) placed on obtaining it. Generically the software is referred to as "RSS"; Radio Service Software. Different versions of it are used for programming different radios. Its almost all entirely written for DOS PCs. The interface between the computer's serial port and a radio is called a "RIB"; Radio Interface Box. Early versions of this circuit were nothing more than a simple "level shifter" which changed the PCs RS232 voltages to something

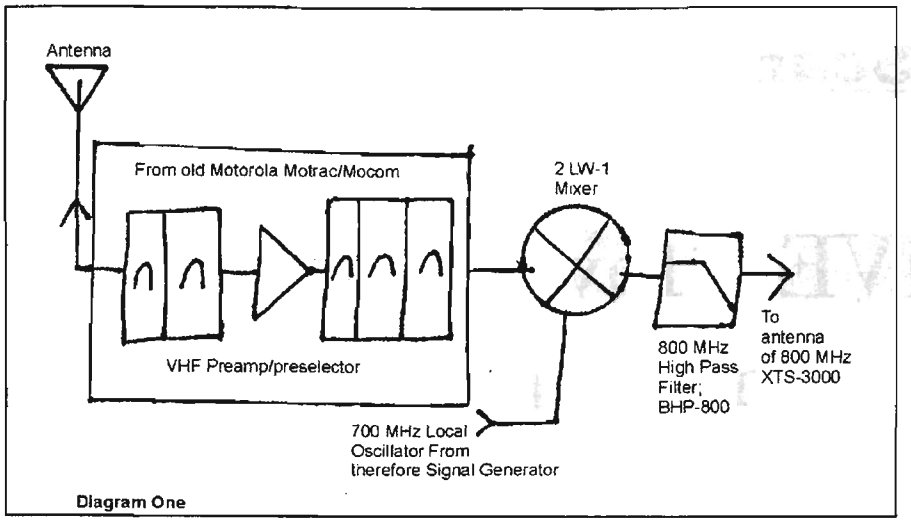

Diagram One

compatible with a radio's microcontroller chip. A newer version of the RIB is something called a "Smart RIB", which can be used with many of Motorola's newer radios that have the "flashport" option which permits the radio's entire operating system firmware to be updated as new versions become available to enable the radio to have improved performance and new features. The Smart RIB may also act as a form of data "buffer", making for more reliable transfers of normal programming data between the radio and a PC. Circuit diagrams for the basic RIB can be found on a couple of different Internet sites.

Learning how to use the Motorola RSS can be a bit tricky as you get used to the "tree" structure of the DOS program. However RSS is richly endowed with Help menus that explain certain things. One thing that you may want to look for that can help with your understanding of programming Motorola radios is the manuals that go along with certain versions of the software. These can often be found for sale online and at some Ham fleamarkets. The manual that covers most of the Astro radios is RVN4100, part number: 6881074C70x, where "x" is the revision letter; "L" appears to be the latest, where as one from 1997 would be an "F".

There are a number of "Motospeak" terms that you should be familiar with as you learn about Motorola radio programming. One is a thing called a "Codeplug". This is actually the entire data file that is programmed in to and retreived out of the radio. Not only does it contain the frequency and subaudible tone data, but also things such as information on different options installed in the radio and the model ID which defines how many channels the radio can have and over what frequency range too. The Term Codeplug, I believe, goes back to the very first generation of Motorola radios(and pagers) that were programmed by way of a small plugin module that contained a PROM or EPROM with all of the associated programming data on it.

Another common term that you will quickly get familiar with is, "Personality". Within the programming software, Motorola radios don't have specific channels, you have a "personality". A personality is a file that you create which calls out a certain receive and transmit frequency, along with things like subaudible tones. You then can use a selected group of personalities to form a specific batch of channels within a "Zone" or otherwise known as a "bank" or "group". Although it takes a bit to get used to, it's the format that actually makes programming large numbers of frequencies easier and flexible.

After performing some the various test we needed to do on the XTS3000 portables, I started to wonder as to whether or not it might just be possible to use one to decode the Astro signals from the NH State Police. Even with the programming software available, this would not be a "plug and play" procedure, as the radios I had were meant for 800 MHz operation, and the NHSP radio system was on 150 MHz. So, being the ever resourceful "hacker" I got the idea to bolt together a simple, external, frequency "up converterer", See diagram 1. This consisted of a Mini Circuits mixer module and a preamp/preselector out of an old Motorola Mocom radio(I think).

We also included a Mini Circuits 800 MHz High Pass filter between the mixer and the XTS's antenna, just for good measure. The RF for the Local Oscillator was supplied from the signal generator output of my Service Monitor, with its frequency calculated so as to up convert the VHF, 151.400 MHz signal from the local State Police repeater, to one of the 853 MHz channels that we had programmed into the XTS. To say the least I was completely thrilled when I first heard the sound of regular human voice coming from the XTS's speaker instead of the usual hiss/buzz of the Astro encoded signal.

One small glitch that we did encounter with all of this was that initially we were able to get the XTS to automatically unmute it's audio. We needed to manually press the Monitor button on the side of the radio in order to activate the speaker. So we went back and looked in the programming manual and software for some answers and this is what we found: Astro/ digital signals do not make use of conventional PL/DPL codes, they have instead what is referred to as Network ID codes.

This is a three digit Hexadecimal number that functions in basically the same way as a PL/DPL code; it provides a way for different user groups on a radio system to only hear signals intended for their group. It also provides a way to selectively access the inputs to repeaters at different locations. We also learned there was a simple way around using the Network ID code, by merely selecting what is called DSQ (Digital SQuelch). This setting allows the radio's receiver to unmute when it detects ANY valid Astro signal. After correcting this function in the radio's "personality" programming, the XTS worked was though it was receiving any other "normal" analog signal.

Understanding the role of the Network ID code was very significant as this means there is NO secret code(s) needed in order to monitor an Astro, or assumably any other APCO Project 25 radio system. You merely need a radio that has the correct internal firmware for the type of system that you are monitoring. I had previously been under the impression that you needed some form of "address key" in order to decode a digital signal. This may or may not be true with respect to monitoring digitally encoded signals that are part of a "trunked" radio system, but we already know that you don't need the so called "system key" in order to track various groups/fleets that occupy a trunked network by using a PC along with a program like Trunker.. True, there are some situations where some digital radio systems will go on to use encryption. But the simple fact still remains that encryption scramblers are an HARDWARE "add on" option which co$t extra, and add little or nothing to the actual performance of a radio.

In listening to the activities on the local State Police Astro repeater over the course of several days, among other things we noticed was that Troopers will sometime converse to each other(car to car) on the repeater output, instead of going off to a separate channel. And perhaps the most interesting was that even with the use of digital modulation that prevent (almost) anyone except their own people from monitoring their radio transmissions, the Dispatchers still regularly ID with their FCC call sign of: WPBC524. Remember, for the very latest in digital scanning news, stay right here with *Scanning USA*.