

Some Thoughts on Software Defined Radios

Michael J. Marcus

The topic of software defined radios (SRD) was first raised by the MMITS Forum. (see www.mmitsforum.org) The question was motivated by the issue of transceivers which are implemented in digital signal processing hardware with significant software components. By changing such software it is possible to significantly change the characteristics of the transceiver such as frequency, power, modulation, bandwidth and protocol. For example, Watkin-Johnson has been manufacturing for several years now the WJ-870 series of HF receivers (see http://www.wj.com/prodinfo/tgprod/hf_vhf_uhf_Rec/8710_11a_12a.html). Most of the receiver functions are implemented in DSP including demodulation and most of the filtering. While this is an HF receiver, the extension of these concepts to practical transceivers at higher bands is just a matter of time.

However, the use of such technology in transceivers for the commercial market raises several new policy issues. If these issues can not be solved within the next year or two, it may delay the introduction of this promising technology. In addition, the same issues may be forcing manufacturers of today's technology to design, manufacture, and stock multiple models of very similar equipment mainly to satisfy existing regulations.

A somewhat similar policy issue arose in the US about a decade ago when several Japanese manufacturers introduced transmitters with frequency synthesizers instead of the traditional crystal control technology. These were marketed without major policy change, but this marketing was challenged by a major user group that was concerned that such radios might be easily programmed for interference on unauthorized channels, particularly public safety channels. Thus there was some uncertainty in marketing such systems for about a year while new rules were developed. These were codified at 47 CFR 90.203(e)-(g).

A similar rule was developed later for marine transmitters, 47 CFR 80.203(b). While these rules are similar, they are not the same and both have loopholes which permit the marketing of radios which are too readily modified.

A related problem involves amateur radio transmitters which are not subject to equipment authorization in the US. For several years manufacturers sold transmitters that had synthesizers and could be readily tuned outside amateur bands. FCC staff action finally stopped this practice, but it is unclear how robust to tampering such amateur transmitters must be.

We may be able to learn from this experience in playing catch up in the case of the introduction for synthesizer technology, to consider cooperation with industry in developing guidelines for SDR in order to remove unnecessary regulatory barriers to the introduction to this technology and maintain a "level playing field" with respect to traditional technology.

Today's equipment authorization policies in the US, Japan, and elsewhere assume that a piece of *hardware* is tested for compliance and that once it is tested, siblings off the production line will be similar. However, with SDR much of this has changed. Loading new software can radically change the performance of the radio after manufacture. This, of course, is the promise and hope of SDR, but it is a dual edged sword. Unauthorized software, perhaps readily distributed by internet, should result in radios that transmit in unauthorized bands, intercept unauthorized frequencies, have protocols that cause interference, etc. Thus they could be a significant threat to order in various radio bands.

Lest this seem to theoretical, it is worthwhile to note that a black market has developed in California for automobile engine control computer ROM chips that boost car performance – presumably at the expense of California clean air standards. (see <http://www.dinabmw.com/html/chips.html>)

I suggest that regulatory agencies try to develop policy that gives reasonable confidence that new radios using hardware and software are compliant with relevant equipment authorization rules. But “reasonable” I suggest that the security of today's hardware only systems be set as a milestone. Today's systems can be modified to yield non-compliant hardware, but it is challenging for the average user. We don't want software radios that can be modified as easily as today's car engine control computers.

Today's hardware radios are both somewhat hard to modify and have a physical label which shows that the radio has passed equipment authorization and the type of use it is authorized for. I suggest that system for SDR might include provisions for both functions.

Equipment authorization authorities could certify combinations of software and hardware for compliance with relevant rules using basically the same approach as used in today's testing. Then the software could be “sealed” to prevent tampering. We could require that approved hardware must check the “seal” to check it is authentic before using the software.

Fortunately, technology is at hand which can check the “seal” and authenticate software as being properly certified. Such technology can be made nearly tamperproof. Such authentication systems work by computing a parity check of the software, such as with a convolutional coder, and then encrypting the parity check. The software is verified by doing the same parity check before using the software and checking it with the encrypted information. If a “trap door code” is used, it is possible to check the data without having the ability to produce new encrypted parity checks. Thus the hardware can check validity but can not forge the authentication of other software.

If such an approach is used, regulatory agencies must decide what type of authentication algorithm is appropriate and what should be the cryptographic key distribution system for the parity bit encryption that prevents unauthorized parties from computing valid sequences for unauthorized software. For example should all manufacturers have access to the cryptographic keys or only equipment certifying authorities?

The other issue is checking what software is loaded into the radio. Today's analogous task is checking the physical authorization label on the radio. I propose that rules for SDR require that an inventory of loaded software and its version number must be accessible from the normal control panel using either a clearly labeled key or a standard procedure so that any radio inspector can audit the contents of a radio. (This function would probably also be useful to maintenance personnel and users.)

While MMITS is focusing on sophisticated radios with multiple features suitable for carrier-provided services such as cellular, PCS, PHS and IMT2000, such concepts might be extended to a much simpler transmitter similar to models already marketed. For example, today's VHF land mobile radios, VHF marine radios and amateur 2 meter radios are really almost identical hardware. (Actually in the US market there are both Government and Non-Government band VHF landmobile radio models with slightly different bands and channel spacing.) Several manufacturers make all these types and then make different variants for the Japanese domestic market, US market, and European market. Each requires a different model, different production, separate shipping and inventory for distribution. This increases the cost for the manufacturers and users. The use of the above concepts could allow a common production run for all these models with software customization at the point of sale. It might also allow users with a legitimate need for multiple radios to use multiple software in the same hardware.

As MMITS technology becomes practical, more sophisticated radios could enter the marketplace and compete on their merits. In the case of carrier-provided services these radios might even allow over-the-air loading of software for the new features.

An interesting regulatory advantage of SDRs is that they could make changes in channel width, modulation, and band plan much more practical for mobile users, much more practical as software for both the new system and the old system could be loaded in advance of a transition and then enabled at the transition time. This is much easier than installing new radios in anticipation of a change, then operating old radios up to the moment of transition, and then removing old radios after the transition.