April 22, 2010

Correspondence Reference Number: 38752

Dear Mr. Bonilla,

You have requested that we submit more detailed information regarding the methods used to ensure requirements in Part 15.212(a)(2)(iv): *"How will manufacturers keep track of the control software? What manufacturing procedures and/or steps were taken to prevent any third party from modifying the control software parameters? "*

In the documentation submitted earlier we explained the following: "*Only the transmitter control element and the RF front-end approved can operate together. Both elements are permanently soldered on the mother board of the host device and cannot be replaced by the user. The firmware in the control element is read/write protected memory. The MCU firmware/software that determines the data rate, the contents of the data packet and the duration of transmission is stored in non-volatile (FLASH) memory on the MCU. The memory on the MCU is read/write protected by the manufacturer so it cannot be accessed by the user or any other party for any unauthorized modifications of transmitter parameters*"

We also stated: "*The X4USPC Limited Split Modular transmitter is not intended for marketing and distribution as a stand alone module. The components of the Limited Split Modular transmitter are permanently affixed to a mother board of the host device. The host device and the Limited Split Modular transmitter are produced and installed by the same manufacturer and only by that manufacturer*."

With above stated, I cannot see how a third party could modify the control software parameters more than they could on any other wireless product on the market. Here are a few reasons as to way a third party would not modify the software parameters or the hardware configuration:

1. The cost of the system to a third party is close to $1,000. The value of the device is inherently due to its application specific feature and NOT necessarily in being wireless. There are many cheaper part 15.231 remote control products available on the market.
2. The application specific features which account for the device's added value are implemented in software and integrated with the transmitter control software parameters in the same program memory on the microcontroller.
3. No third party has access to the source code which is the intellectual property of the manufacturer. Without the source code it is virtually impossible to understand what part of the compiled binary or hex data does. However, to prevent any unauthorized access to the compiled code, the manufacturer has set code protection of the program memory in the microcontroller so it cannot be read by a third party.
4. Thus, any write to the program memory requires that the entire memory will be erased causing the loss of both application specific and transmitter control software and rendering the device inoperable. In fact, due to its unique microcontroller controlled power supply system the device will not even turn on.
5. To reprogram the microcontroller for transmitting via the RF front-end, a third party would need to figure out the electrical schematic (which is not available to the public), have excellent knowledge of the microcontroller and the RF front-end and develop the control software from scratch.
6. Therefore, if a third party had such capabilities, one would assume that they could "hack" almost any software controlled transmitter device on the market and modify its control parameters. The reality however, is that entities with such capabilities develop their own products for their specific requirements and at much lower cost then buying an expensive application specific device and "hacking" it.

Sincerely,
Barak Dar
SoundGate, Inc