Telemetry Receiver
SRX800

FCC Statements

Lotek Wireless
115 Pony Drive
Newmarket, Ontario
Canada, L3Y 7B5

Tel: 905-836-6680
Fax: 905-836-6455
Web-site: www.lotek.com

1. The SRX800 receiver has extensive safeguards to prevent the unauthorized reception of cellular telephone voice and data signals. The same measures prevent an unauthorized and illegal attempt to modify the device for such a purpose:

◊ The high Q band-pass filters on the front end of the RF receiver are tuned to the VHF band (e.g.150 MHz) band and offer 30 dB rejections each of out-of-band signals, including the cellular frequencies. The cellular band is far from the SRX reception band and so the cellular signals will be greatly attenuated by as much as 60 dB.

◊ The 12 MHz crystal filter after the synthesizer offers additional selectivity and permits only 8 kHz bandwidth signals through. Since the cellular signals have a 30 kHz bandwidth, even if they pass through the narrower IF filter they would be weakened & distorted.

◊ The SRX demodulator is designed to receive on-off keying modulation. Since cellular phones use FM modulation they will not be demodulated by the SRX receiver.

◊ Due to the embedded firmware, cellular frequencies, or any other parameter which would be relevant to a cellular RF signal cannot be entered into the keypad, neither can they be entered through any other method. Only valid frequencies belonging to the frequency range (VHF band) of the receiver can be entered.

◊ Access to the internal resident firmware is practically impossible. Removing the chips or other elements of the circuitry would practically compromise the whole functionality of the unit. Furthermore, the firmware is strongly customized for this type of receiver, which significantly adds to its security. In addition, any entry is pass-word protected.

◊ Mechanically, the SRX 800 system consisting of the CPU board, the RF board, and the interconnect board, is enclosed in a solid enclosure, and inside access is extremely difficult, should anyone attempt modifications.

2. The telemetry receiver was designed to make any alteration of the tuning, filtering and control inaccessible:

◊ The receiver is configured at factory site. The keypad does not allow the entering of different parameters than the allowed ones. Neither does it allow entering such control or filtering functions. These functions are determined by the hardware and by the firmware. Both the CPU board and the VHF board are controlled by firmware, which prevents any alteration of the original functionality of the receiver.

◊ Any access to the internal resident firmware is practically impossible.

3. The telemetry receiver was designed to make any alteration impossible by an unauthorized person, without making the device inoperable:

◊ The circuitry located inside is practically inaccessible to a potential intruder, due to the ruggedized casing.

◊ Removing the chips or other elements of the circuitry would practically compromise the whole functionality of the unit.

◊ The firmware is strongly customized for this type of receiver, which significantly adds to its security. In addition, any entry is pass-word protected.