Wireless Telecom Group
Boonton Microlab Noisecom

25 Eastmans Road
Parsippany, New Jersey 07054

Boonton 55-Series Wideband USB
Peak Power Sensor Security Procedures

Product Name: Boonton 55-Series USB Peak Power Sensor

Applicable Models: All 55xxx USB power sensors

1. **Memory Description.** The Boonton 55-Series power sensors contain three types of internal memory, designated (a) through (c). A discussion of each memory group follows.

   a. Program/Data Flash

   i. Type/Model: Non-volatile SPI Flash, S25FL128S
   ii. Size/Org: 128 Mbit (16 Mbyte serial QSPI)
   iii. Location: U12 on main control board
   iv. Contents:
   - Bootloader image (executable software): primary and backup
   - Main application image (executable software): primary and backup
   - FPGA image (data tables): primary and backup
   - Factory identification and configuration tables (model, s/n, etc)
   - Sensor calibration tables (factory and/or authorized calibration lab)
   - User calibration table (field generated): zero and fixed cal factors
   - Unused area

   v. Read Access:
   - No documented read methods are available to the user.
   - Read by main CPU to boot and execute sensor bootloader, load main sensor application, load FPGA system, and access sensor calibration tables.
   - No external read access is performed during normal operation.
   - Limited external read access is performed during firmware update and calibration data entry.
   - Possible to read externally with software development system by opening sensor and connecting to pcb with proprietary programming cable and pod.

   vi. Write Access:
   - No documented write methods are available to user.
   - No write access occurs during normal operation.

- Written by main CPU under external control during firmware update and calibration data update.
- Can be written externally with software development system by opening sensor and connecting to pcb with proprietary programming cable and pod.

vii. Sanitization:

- Not typically necessary since no user info is automatically saved.
- If required, an external "data wipe" procedure may be used to erase a selected portion of the flash. Partial erasure may require reprogramming of some or all firmware and some or all calibration data.
- If required, an external "flash wipe" procedure may be used to erase the entire flash memory. Full erasure will render the instrument inoperative, and factory reprogramming and recalibration will be necessary.

b. Program/Data RAM

i. Type/Model: On-chip volatile static RAM
ii. Size/Org: 256 kbytes (four 64 kB banks)
iii. Location: U11 on main control board
iv. Contents: Main program and all temporary program and user data
v. Read Access: Main CPU during program execution. Not directly user accessible.
vi. Write Access: Main CPU during program execution. Not directly user accessible.
vii. Sanitization: All data is destroyed by unplugging sensor for 15 seconds.

c. FPGA acquisition/buffer RAM

i. Type/Model: FPGA volatile Block RAM
ii. Size/Org: Approx 5 Mbits in various areas and organizations
iii. Location: U11 on main control board
iv. Contents: Acquisition data, working cal tables, measurement output buffers
v. Read Access: FPGA and main CPU. Not directly user accessible.
vi. Write Access: FPGA and main CPU. Not directly user accessible.
vii. Sanitization: All data is destroyed by turning off instrument for 15 seconds.

2. **Sanitization Discussion.** Data in the volatile CPU Program/Data RAM and FPGA block RAM will be destroyed ("sanitized") by removing power from the sensor for 15 seconds. All user-set setup and configuration data as well as any buffered measurement data is contained in the volatile memories, and will be cleared upon power loss. The sensor contains no internal power source, so unplugging the sensor's USB connection will sanitize all volatile memory within the power sensor.

   Data in the non-volatile Program/Data Flash consists only of permanent identification and calibration information. Measurement settings, configuration or acquired measurement data cannot be stored in the non-volatile memory, so sanitization of this area is typically unnecessary.

   - User sensor calibration ("fixed cal" or "zero") offset values can be stored to a dedicated area "user calibration" area of the Program/Data Flash. Only the actual offset correction values are stored, and this occurs only in response to explicit user commands. No measurement or configuration data is stored, so these functions should pose minimal security risk.
   - It is possible, although extremely unlikely, that a specialized remote application could write data into free areas of the Program Flash via the instrument's USB connection. The procedures for doing this are not available to users, but could possibly be "hacked" by a highly skilled and determined individual. Doing so would require detailed knowledge of the instrument's architecture and memory map which are maintained as proprietary Boonton information. This would allow a several megabytes of arbitrary data to be concealed in free areas of the memory device.

     If this issue is considered a security concern, a data wipe procedure can be used to wipe/erase some or all data within the Program/Data Flash (see above). *Following this action, service procedures will then be required to restore proper sensor operation.*

Sanitization Procedures. Any or all of the following three steps may be used to sanitize instrument memory. The steps are listed in order of data security from lowest to highest.

a. **User Cal/Zero Data**: The sensor's user cal/zero data should not be a security issue, but if it is, perform a fresh cal or zero from the API or other application.

b. **Volatile Data:** All volatile data including all measurement data may be cleared by disconnecting the sensor from the USB for 15 seconds.

c. **Program/Data Flash**: Consult factory for Erase/Wipe utility.