25 Eastmans Road
Parsippany, NJ 07054 USA

Boonton 4530 Series Instrument Security Procedures

This discussion covers the following Boonton Electronics models: 4531 and 4532 RF Power Meters.

1. **Memory Description.** The Boonton 4530 Series instruments contain seven types of internal memory, designated (a) through (e). A discussion of each memory group follows.

a. Program Flash

i. Type/Model: Non-volatile NOR Flash, 28F040
ii. Size/Org: 4Mbit (512Kx8x2)
iii. Location: U43/U44 on main control (upper) pc board.
iv. Contents: The program flash is blocked into the following sections:
    1. Bootloader image (executable software)
    2. Main application (executable software)
    3. DSP image (executable software)
v. Read Access: Main CPU to boot and execute instrument application and load DSP system. Not user accessible. Flash chips can only be read by removing from socket and using an external programmer.
vi. Write Access: No documented write method is available to the user. The flash can be written during firmware update, but only with special programming software. Flash chips can also be written by removing from socket and using an external programmer.
vii. Sanitization: Not necessary. If needed, U43 and U44 may be removed from sockets and externally erased. This will render the instrument inoperative.

b. NVRAM

i. Type/Model: Battery backed-up SRAM, CY62256LL or equivalent
ii. Size/Org: 256Kbit (32Kx8)
iii. Location: U18 on main control (upper) pc board.
iv. Contents: The NVRAM is blocked into the following sections:
    1. Sensor “autocal” files (system created linearity correction files which typically contain no classified user measurement or setting data).

2. Most recent (or "current") instrument setup configuration (system created settings file placed into user preset location 0).
3. User-saved instrument setup configurations (system created settings files placed into user preset locations 1 to 4).

v. Read Access: Main CPU for recalling saved instrument data. Not directly user accessible, but current configuration settings may be individually read by user.

vi. Write Access: Main CPU for saving instrument data. Written to save user cal info, user setups or current configuration settings. It is not possible to directly write arbitrary user data.

vii. Sanitization: With instrument power OFF, short U18-pin 28 (NVRAM Vcc pin) to ground for 5 seconds. This removes battery power and the SRAM will "forget" any saved data. Alternatively, writing default data into the "working" memory location and into each of the user preset locations 1-4, as described in section 3.c, will remove any unique user data that may be classified.

c. Host Processor RAM

i. Type/Model: Volatile Static RAM, CY7C1009 or equivalent
ii. Size/Org: 256Mbit x 4 (16Mx16x2)
iii. Location: Main instrument (upper) pc 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 turning off instrument for 15 seconds.

d. Configuration EEPROM

i. Type/Model: Non-volatile EEPROM, 24C128 or equivalent
ii. Size/Org: 128kbit (16Kx8)
iii. Location: Main instrument (upper) pc board.
iv. Contents: Permanent configuration data, semi-permanent calibration data.
v. Read Access: Main CPU to recall factory configuration and calibration data.
vi. Write Access: Main CPU to store factory configuration and calibration data.
vii. Sanitization: None. Data must be preserved for correct instrument operation.

e. DSP program/acquisition RAM

i. Type/Model: Volatile Static RAM, CY7C1009 or equivalent
ii. Size/Org: 256Mbit x 4 (16Mx16x2)
iii. Location: DSP (lower) pc board.
iv. Contents: DSP program and data, and sample acquisition data
v. Read Access: DSP during program execution. Not directly user accessible.
vi. Write Access: Main CPU during DSP program load, and DSP during DSP program execution. Not directly user accessible.
vii. Sanitization: All data is destroyed by turning off instrument for 15 seconds.

2. **Sanitization Discussion.** Data in the Host Processor RAM and DSP RAM will be destroyed ("sanitized") by removing power from the instrument for 15 seconds. Data in the Program Flash and Configuration EEPROM is permanent factory data and does not require sanitization. The only security concern is data in the NVRAM, which saves configuration and user calibration information.

   User sensor calibration ("autocal") files and saved instrument setups are stored in an area of the NVRAM. There is no menu procedure for erasing this data, but these locations may be overwritten with fresh data via the procedure below. Alternatively, the entire NVRAM can be cleared by shorting its Vcc pin to ground. Either of these methods should meet most security concerns.

   The three program images (bootloader, main application, and DSP application) are stored in their own area of the Program Flash. This area can only be written during a firmware update procedure – a process which loads data from a remote computer into the flash memory of the instrument.

   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 RS232. 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 small amount of arbitrary data to be concealed in free areas of the memory devices.

   And since the chips are socketed, it is also possible that a user could remove them and write additional data into free areas. This would require opening the instrument case, which would break the plastic film security seal.

   If either of these issues is considered a security concern, both flash chips can be removed from their sockets and erased or destroyed before the instrument is removed from a secured area. This will render the instrument totally inoperative and require a factory service procedure to repair.

Alternatively, the two chips (U43 and U44) could be duplicated before the instrument enters a secure area, and the two sets may be kept inside and outside the area. However, the sockets used on the main pc board are designed only for occasional use, so removing and re-inserting chips may wear the contacts and cause reliability issues after a dozen or so cycles.

3. **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. **Autocal Data**: The sensor autocal files (linearity correction data – one per channel) do not contain classified data and are not typically a security concern. If desired, the Calibration menu allows erasing the file for each channel (Cal/Zero > Cal Cancel).

   b. **Volatile Data:** All volatile data including all measurement data may be cleared by turning off instrument power for 15 seconds. Note that the current instrument configuration (all of the front panel settings) is preserved and will be restored when power is re-applied.

   c. **Saved User Setups**: All saved user setups and the saved "current state" may be cleared by recalling instrument default settings (Main Menu > Defaults) to update the "current state", then selecting each of the 4 User Preset locations (Main Menu > Save/Recl > SetupSave) in sequence and saving the current (default settings) state to that location:

      i. Main Menu > Defaults — Loads Preset 0 with default settings
      ii. Main Menu > Save/Recl > SetupSave > 1 — Loads Preset 1 with current defaults
      iii. Main Menu > Save/Recl > SetupSave > 2 — Loads Preset 2 with current defaults
      iv. Main Menu > Save/Recl > SetupSave > 3 — Loads Preset 3 with current defaults
      v. Main Menu > Save/Recl > SetupSave > 4 — Loads Preset 4 with current defaults

      Note that certain non-measurement (unclassified) configuration settings such as the communication, and display settings will be preserved.