25 Eastmans Road
Parsippany, NJ 07054 USA

Boonton 4540 Series Instrument Security Procedures

This discussion covers the following Boonton Electronics models: 4541 and 4542 RF Power Meters.

1. **Memory Description.** The Boonton 4540 Series instruments contain seven types of internal memory, designated (a) through (g). A discussion of each memory group follows.

   a. Boot Flash

   i. Type/Model: Non-volatile NOR Flash, 28F160
   ii. Size/Org: 16Mbit (1Mx16)
   iii. Location: Single board computer module mounted on instrument main pc bd.
   iv. Contents: Permanent boot loading software
   v. Read Access: Main CPU to boot/execute startup program. Not user accessible.
   vi. Write Access: Factory only, using external programmer.
   vii. Sanitization: Not necessary or possible.

   b. User Flash

   i. Type/Model: Non-volatile NOR Flash, 28F256
   ii. Size/Org: 256Mbit (16Mx16)
   iii. Location: Single board computer module mounted on instrument main pc bd.
   iv. Contents: The user flash is blocked into the following sections:
      1. Main 4540 application (executable software)
      2. DSP image (executable software)
      3. FPGA configuration image (binary data)
      4. Sensor “autocal” files (system saved files)
      5. Most recent setup configuration (system saved file)
      6. User-saved instrument setups (system saved files)
   v. Read Access: Main CPU for updating software images and system/user files. Not directly user accessible, but current configuration settings may be individually read by user.
   vi. Write Access: Main CPU for loading software images and user data. Written to install new software, or to save user cal info, user setups or current configuration settings.
   vii. Sanitization: Any or all sections may be erased via front-panel procedures.

c. Main System RAM

i. Type/Model: Volatile DDR SDRAM, MT46V16M16
ii. Size/Org: 256Mbit x 4 (16Mx16x2)
iii. Location: Single board computer module mounted on instrument main pc bd.
iv. Contents: 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. Video Display Buffer

i. Type/Model: Volatile VRAM, SM712C
ii. Size/Org: 16Mbit (2Mx8)
iii. Location: Single board computer module mounted on instrument main pc bd.
iv. Contents: LCD display screen image data.
v. Read Access: LCD display controller to refresh screen image.
vi. Write Access: Main CPU to create screen image.
vii. Sanitization: All data is destroyed by turning off instrument for 15 seconds.

e. Configuration EEPROM

i. Type/Model: Non-volatile EEPROM, 24C128
ii. Size/Org: 128kbit (16Kx8)
iii. Location: Main instrument 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.

f. Acquisition Buffer

i. Type/Model: Volatile Static RAM, GS74116
ii. Size/Org: 4Mbit, (256Kx16x2)
iii. Location: Main instrument pc board.
iv. Contents: Acquired measurement sample data
v. Read Access: Read by DSP to retrieve buffered measurement data
vi. Write Access: Written by hardware to buffer acquired measurement data

vii. Sanitization: All data is destroyed by turning off instrument for 15 seconds.

g. Main DSP RAM

i. Type/Model: Volatile SDRAM, 6MT48LC16M4
ii. Size/Org: 4Mbit x 2 (16Mx4x2)
iii. Location: Main instrument pc board.
iv. Contents: DSP program and data
v. Read Access: DSP to execute DSP application program.
vi. Write Access: Written by main CPU to load DSP program, and by DSP during DSP program execution.
vii. Sanitization: All data is destroyed by turning off instrument for 15 seconds.

2. **Sanitization Discussion.** Data in the Main System RAM, Video Display Buffer, Acquisition Buffer, and Main DSP RAM will be destroyed ("sanitized") by removing power from the instrument for 15 seconds. Data in the Boot Flash and Configuration EEPROM is permanent factory data and does not require sanitization. The only security concern is data in the User Flash, which functions as a disk drive.

   User sensor calibration ("autocal") files and saved instrument setups are stored in an area of the User Flash which is configured as a disk drive. This area may be erased via a menu procedure which erases all stored user data and re-initializes the flash disk. This meets most security concerns.

   The three program images (main application, DSP application, and FPGA configuration data) are stored in their own area of the User 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 the program area of the User Flash. For this reason, a procedure is available to erase the ENTIRE user flash, including all of the program images. Use of this procedure will render the instrument inoperative until the firmware is re-installed. Field firmware installation may be performed via Ethernet connection using the standard 4540 firmware update utility.

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. **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.

b. **Saved User Setups**: Most saved user setups and the saved "current state" may be cleared by recalling instrument default settings (Setup > Defaults > Load), then selecting each of the 25 User Preset locations (Setup > User Presets > Preset Name) in sequence and deleting each one (Setup > User Presets > Preset Delete). Note that certain non-measurement configuration settings such as the communication, and display settings will be preserved.

c. **Entire User Data Area**: The user data area of the instrument is configured as a flash drive and may be erased by first enabling service mode (System > Servicing > Svc Cal Mode ON), then selecting Security > Erase User Data and confirming at the prompts. The entire flash drive, including all settings, saved setups and saved autocal data will be erased. Factory calibration and configuration data is preserved.

d. **Entire User Flash Chip**: The entire user flash chip may be erased by first enabling service mode (System > Servicing > Svc Cal Mode ON), then selecting Security > Erase All Memory and confirming at the prompts. The entire user flash chip including all user data and all instrument firmware will be erased. Factory calibration and configuration data is preserved.

Note that steps 3b through 3d are additive – that is each step includes the functions of the steps above it. If step 3c is performed, it is not necessary to perform step 3b. If step 3d is performed, it is not necessary to perform steps 3b or 3c.

If steps (3a and 3d) have been performed, the only data which will remain in the instrument is the factory bootload firmware in the Boot Flash (needed to re-install the application firmware), and the factory configuration and calibration data in the Configuration EEPROM. Since neither of these areas may be written by the user, the instrument may be considered secure.

Note: Sanitization methods 3c and 3d are not implemented in 4540 firmware releases prior to 20090305.