ESG/PSG Security Features

This document applies to the following Agilent signal generators:

ESG Models	E4428C (firmware revision - all) E4438C (firmware revision ≥ C.03.40)
PSG Models	E8247C (firmware revision ≥ C.03.40) E8257C (firmware revision ≥ C.03.40) E8267C (firmware revision ≥ C.03.40) E8257D (firmware revision - all) E8267D (firmware revision - all)

Agilent Technologies

Part Number: E4400-90621

Printed July 2005

Using Security Functions

This section describes how to use the ESG/PSG security functions to protect and remove classified proprietary information stored or displayed in the instrument. All security functions described in this section also have an equivalent SCPI command for remote operation. (Refer to the “System Commands” chapter of the *SCPI Command Reference* for more information.)

Understanding Memory Types

The ESG/PSG comprises several memory types, each used for storing a specific type of data. Before removing sensitive data, it is important to understand how each memory type is used in the signal generator. The following tables describe each memory type used in the base instrument, optional baseband generator, and optional hard disk.

Table 0-1 Base Instrument Memory

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks
Main Memory (SDRAM) 64 MB	Yes	No	firmware operating memory	operating system (not user)	CPU board
Main Memory (Flash) 20 MB	Yes	Yes	factory calibration/ configuration data user file system, which includes flatness calibration, IQ calibration, instrument states, waveforms (including header and marker data), modulation definitions, and sweep lists	firmware upgrades and user-saved data	CPU board (same chip as firmware memory, but managed separately) User data is not stored in this memory if hard disk (Option 005) is installed. Because this 32-MB memory chip contains 20 MB of user data (described here) and 12 MB of firmware memory, a full-chip erase is not desirable. User data areas are selectively and completely sanitized when you perform the **Erase and Sanitize** function.

Table 0-1 Base Instrument Memory

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks
Firmware Memory (Flash) 12 MB	No	Yes	main firmware image	factory installed or firmware upgrade	CPU board (same chip as main flash memory, but managed separately) During normal operation, this memory cannot be overwritten. It is only overwritten during the firmware installation or upgrade process. Because this 32-MB memory chip contains 20 MB of user data and 12 MB of firmware memory (described here), a full-chip erase is not desirable. User data areas are selectively and completely sanitized when you perform the **Erase and Sanitize** function.
Battery Backed Memory (SRAM) 512 kB	Yes	Yes	user-editable data (table editors) last instrument state and last instrument state backup	firmware operations	CPU board The battery can be removed to clear the memory, but must be reinstalled for the instrument to operate. The battery is located on the motherboard for the ESG and on the CPU board for the PSG.
Bootrom Memory (Flash) 128 kB	No	Yes	CPU bootup program and firmware loader/updater	factory programmed	CPU board During normal operation, this memory cannot be overwritten or erased. This read-only data is programmed at the factory.
Calibration Backup Memory (Flash) 512 KB	No	Yes	factory calibration/ configuration data backup no user data	factory or service only	motherboard

Table 0-1 Base Instrument Memory

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks
Boards Memory (Flash) 512 Bytes	No	Yes	factory calibration and information files, code images, and self-test limits no user data	factory or service only	all RF boards, baseband generator, and motherboard
Micro-processor Cache (SRAM) 3 kB	Yes	No	CPU data and instruction cache	memory is managed by CPU, not user	CPU board

Table 0-2 Baseband Generator Memory (Options 601 and 602)

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Remarks
Waveform Memory (SDRAM) 40–320 MB	Yes	No	waveforms (including header and marker data) and PRAM	normal user operation	User data is completely sanitized when you perform the **Erase and Sanitize** function.
BBG Firmware Memory (Flash) 32 MB	No	Yes	firmware image for baseband generator	firmware upgrade	

Table 0-2 Baseband Generator Memory (Options 601 and 602)

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Remarks
Coprocessor Memory (SRAM) 32 MB	Yes	No	operating memory of baseband coprocessor CPU	During normal operation, some user information, such as payload data, can remain in the memory.	This memory is used during normal baseband generator operation. It is not directly accessible by the user.
Buffer Memory (SRAM) 5 x 512 kB	No	No	support buffer memory for ARB and real-time applications	normal user operation	This memory is used during normal baseband generator operation. It is not directly accessible by the user.

Table 0-3 Hard Disk Memory (Option 005)

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Remarks
Media Storage (Built-in Hard Disk) 6 GB or 10 GB (4 GB usable in both cases)	Yes	Yes	user files, including flatness calibrations, IQ calibration, instrument states, waveforms (including header and marker data), modulation definitions, and sweep lists	user-saved data	The magnetic residue requires several rewrite cycles or drive removal and destruction. The hard disk is an option and is therefore not installed in some instruments. If it is installed, these files are stored on the hard disk instead of in flash memory. User data is completely sanitized when you perform the **Erase and Sanitize** function.
Buffer Memory (DRAM) 512 kB	No	No	buffer (cache) memory	normal operation through hard disk	

Removing Sensitive Data from Memory

When moving the signal generator from a secure development environment, you can remove any sensitive information stored in the instrument. This section describes several security functions you can use to remove sensitive data from your instrument.

Erase All

This function removes all user files, user flatness calibrations, user I/Q calibrations, and resets all table editors with original factory values, ensuring that user data and configurations are not accessible or viewable. The instrument appears as if it is in its original factory state, however, the memory is not sanitized. This action is relatively quick, taking less than one minute.

To carry out this function, press **Utility** > **Memory Catalog** > **More (1 of 2)** > **Security** > **Erase All** > **Confirm Erase**.

NOTE This function is different than pressing **Utility** > **Memory Catalog** > **More (1 of 2)** > **Delete All Files**, which deletes all user files, but does not reset the table editors.

Erase and Overwrite All

This function performs the same actions as **Erase All** and then clears and overwrites the various memory types in accordance with Department of Defense (DoD) standards, as described below.

SRAM – All addressable locations are overwritten with random characters.
CPU Flash – All addressable locations are overwritten with random characters and then the flash blocks are erased. This accomplishes the same purpose of a chip erase, however, only the areas that are no longer in use are erased and the factory calibration files are left intact.
DRAM – All addressable locations are overwritten with random characters.
Hard Disk – All addressable locations are overwritten with a single character. (This is insufficient for top secret data, according to DoD standards. For top secret data, the hard drive must be removed and destroyed.)

To carry out this function, press **Utility** > **Memory Catalog** > **More (1 of 2)** > **Security** > **Erase and Overwrite All** > **Confirm Overwrite**.

Erase and Sanitize All

This function performs the same actions as Erase and Overwrite All and then adds more overwriting actions. After executing this function, you must manually perform some additional steps for the sanitization to comply with Department of Defense (DoD) standards. These actions and steps are described below.

SRAM – After applying this function, the instrument must remain in the secure area for a period longer than the classified data resided in memory. This measure is necessary to conform to DoD standard 5220.22-M. Alternatively, the SRAM battery can be removed then manually reinserted, however, this requires opening the instrument.
DRAM – All addressable locations are overwritten with a single character. You must then power off the instrument to purge the memory contents.
Hard Disk – All addressable locations are overwritten with a single character and then a random character. (This is insufficient for top secret data, according to DoD standards. For top secret data, the hard drive must be removed and destroyed.)

To carry out this function, press **Utility** > **Memory Catalog** > **More (1 of 2)** > **Security** > **Erase and Sanitize All** > **Confirm Sanitize**.

Using the Secure Mode

The secure mode automatically applies the selected **Security Level** action the next time the instrument's power is cycled.

To set the level of the secure mode, press **Utility** > **Memory Catalog** > **More (1 of 2)** > **Security** > **Security Level** and choose from the following selections:

None – equivalent to a factory preset, no user information is lost
Erase – equivalent to **Erase All**
Overwrite – equivalent to **Erase and Overwrite All**
Sanitize – equivalent to **Erase and Sanitize All**

To activate the secure mode, press **Utility** > **Memory Catalog** > **More (1 of 2)** > **Security** > **Enter Secure Mode** > **Confirm**. The **Enter Secure Mode** softkey changes to **Secure Mode Activated**.

CAUTION Once you select a security level action and activate secure mode by pressing **Confirm**, you cannot deactivate or decrease the security level. The erasure actions for that security level execute at the next power cycle. You can only increase the security level once the secure mode is activated. For example, you can change **Erase** to **Overwrite**, but not the reverse.

NOTE After the power cycle, the security level selection remains the same, but the secure mode is not activated.

If Your Instrument is Not Functioning

If the instrument is not functioning and you are unable to use the security functions, you may physically remove the processor board and optional hard disk, if installed, from the instrument. Once these assemblies are removed, proceed as follows:

For the processor board, choose one of the following options:

- Discard the processor board and send the instrument to a repair facility. A new processor board will be installed and the instrument will be repaired and calibrated. If the instrument is still under warranty, you will not be charged for the new processor board.
- If you have another working instrument, install the processor board into that instrument and erase the memory. Then reinstall the processor board back into the non-working instrument and send it to a repair facility for repair and calibration. If you discover that the processor board does not function in the working instrument, discard the processor board and note that it caused the instrument failure on the repair order. If the instrument is still under warranty, you will not be charged for the new processor board.

For the optional hard disk, choose one of the following options:

- Discard the hard disk and send the instrument to a repair facility. Indicate on the repair order that the hard disk was removed and must be replaced. A new hard disk will be installed and the instrument will be repaired and calibrated. If the instrument is still under warranty, you will not be charged for the new hard disk.
- Keep the hard disk and send the instrument to a repair facility. When the instrument is returned, reinstall the hard disk.

For procedures on removing and replacing the processor board and hard disk, refer to the service guide.

Using the Secure Display

NOTE Front panel control of this feature is *not* available on PSG E82x7C signal generators with firmware revisions earlier than C.03.76. The feature can be activated remotely, however, using SCPI commands. Refer to the "System Commands" chapter of the *SCPI Command Reference* for more information.

This function prevents unauthorized personnel from reading the instrument display and tampering with the current configuration through the front panel. The display is blanked, except for the message `*** SECURE DISPLAY ACTIVATED ***`, and the front panel keys are disabled. Once this function is activated, the power must be cycled to re-enable the display and front panel keys.

To apply this function, press **Utility** > **Display** > **More (1 of 2)** > **Activate Secure Display** > **Confirm Secure Display**

Figure 0-1 ESG/PSG Screen with Secure Display Activated