R&S® ESMD
Wideband Monitoring Receiver
Resolving Security Issues When Working in Secure Areas

4066.5464.02 ─ 01

ROHDE&SCHWARZ

Radiomonitoring & Radiolocation

Resolving Security Issues When Working in Secure Areas

This documentation is valid for the following models and options:

- R&S®ESMD Wideband Monitoring Receiver 4066.0004.02
- R&S®ESMD Wideband Monitoring Receiver 4066.0004.03

Muehldorfstr. 15, 81671 Munich, Germany
Phone: +49 89 41 29 - 0
Fax: +49 89 41 29 12 164
E-mail: info@rohde-schwarz.com
Internet: http://www.rohde-schwarz.com
Printed in Germany – Subject to change – Data without tolerance limits is not binding.

The following abbreviations are used throughout this manual: R&S®ESMD is abbreviated as R&S ESMD.

Contents

1 Overview....5
2 Battery Information....6
3 Types of Memory and their Security Concerns....7
3.1 EEPROM Memory....7
3.2 SDRAM Memory....7
3.3 FLASH Memory....7
3.4 Nonvolatile SRAM Memory....7
3.5 PC EEPROM Memory....8
3.6 PC Bios FLASH Memory....8
3.7 PC SDRAM Memory....8
3.8 PC Removable CompactFlash™ Memory....8
4 Information Storage within the R&S ESMD....10
5 Information Security in Highly Sensitive Areas....11
6 Service, Calibration and Maintenance in Sensitive Areas....12
6.1 Memory Clearing Procedure....12
6.2 Removing the CompactFlash™ Memory....12
6.2.1 Disassembling the R&S ESMD....13
6.2.2 Installing a Compact Flash (CF) Card....15
6.3 Calibration....15
7 Firmware Updates and Backing-Up User Data in Sensitive Areas....16
7.1 Firmware Update via the LAN Interface....16
7.2 GUI Firmware Update via the USB port....16
8 Special Considerations for USB Ports....17

1 Overview

In many cases it is imperative that the R&S ESMD be used in a secured environment. Generally these highly secured environments will not allow any test equipment to leave the area unless it can be proven that no user information will leave with the test equipment. Security concerns can arise when the R&S ESMD needs to leave a secured area to be calibrated or serviced.

This document describes the types of memory and their usage in the R&S ESMD. It also addresses methods of ensuring that no user data will leave the secured area should the product be removed for calibration or service needs.

2 Battery Information

The R&S ESMD is fitted with a lithium backup battery, located on the processor board, for backup of the real time clock, nonvolatile SRAM for receiver settings, memory channel list and suppress list.

3 Types of Memory and their Security Concerns

In the following sections the types of memory and their usage in the R&S ESMD are described. They also address methods of ensuring that no user data will leave the secured area if the product has to be removed for calibration or service needs.

3.1 EEPROM Memory

Each board assembly in the R&S ESMD has one serial EEPROM device. These devices hold 4, 8 or 16 kByte and contain information related to the installed hardware, such as board serial number, options, correction constants, etc. and the LAN settings.

The EEPROM does not hold user data nor can the user access the EEPROM storage.

The EEPROM is not a security concern.

3.2 SDRAM Memory

The R&S ESMD has 512 MByte of SDRAM on the processor board.

SDRAM is volatile memory and it loses its memory as soon as power is removed. The SDRAM will be unreadable within one minute after the power is removed from the device.

The SDRAM is not a security concern.

3.3 FLASH Memory

The processor board in the R&S ESMD has 128 MByte FLASH memory. One part of this FLASH memory contains the firmware (boot program, operating system, application with the default settings) and cannot be accessed by the user.

This part of the FLASH memory is not a security concern.

A second part of the FLASH memory is used as a flash file system which can be accessed by the user via FTP to store antenna correction and antenna factor data.

This part of the FLASH memory may be a security concern if user antenna data has been stored there.

3.4 Nonvolatile SRAM Memory

The R&S ESMD has 2 MByte of battery buffered SRAM on the processor board.

The nonvolatile SRAM contains user settings, the memory channel list and the suppress list.

The nonvolatile SRAM is a security concern.

The nonvolatile SRAM has to be cleared by the Master Preset procedure (see chapter 6.1, "Memory Clearing Procedure", on page 12).

3.5 PC EEPROM Memory

The PC board in the R&S ESMD has one serial EEPROM device. This device contains information related to the installed hardware, such as board serial number and production information.

The EEPROM does not hold user data nor can the user access the EEPROM storage.

The EEPROM is not a security concern.

3.6 PC Bios FLASH Memory

The R&S ESMD model 03 has Bios FLASH Memory on the PC board. This memory contains basic I/O functions and settings and cannot be accessed by the user.

The PC Bios FLASH Memory is not a security concern.

3.7 PC SDRAM Memory

The R&S ESMD model 03 has 512 MByte of SDRAM on the PC board.

SDRAM is volatile memory and it loses its memory as soon as power is removed. The SDRAM will be unreadable within one minute after the power is removed from the device.

The PC SDRAM Memory is not a security concern.

3.8 PC Removable CompactFlash™ Memory

The R&S ESMD model 03 has a removable 4 GByte CompactFlash™ memory. The capacity of the CompactFlash™ memory must be 4 GByte. This CompactFlash™ card is located on the upper right side in the device and can easily be removed after removing the cover.

The CompactFlash™ memory is used to store the

- operating system (Windows XP embedded)
- restore (backup partition)
- GUI firmware

- help system
- user data
  The partition USER (D:] contains the following default subdirectories: Logging, Profiles, Recording, Reports, Snapshot.
  The contents of Logging and Reports can help to analyze hardware or firmware problems and are not a security concern.
  The contents of Profiles, Recording and Snapshot may be a security concern and can be deleted by the user without problems. Another possibility is to remove the CompactFlash™ card.

The CompactFlash™ memory contents are nonvolatile, so nothing is lost when power is removed from the R&S ESMD (see chapter 6.2, "Removing the CompactFlash™ Memory", on page 12) .

The CompactFlash™ memory is not a security concern because it can be physically removed from the R&S ESMD and left in the secure area.

4 Information Storage within the R&S ESMD

Table 4-1: The processor board is equipped in R&S ESMD model 02 and R&S ESMD model 03

Data	EEPROM	SDRAM	FLASH	Nonvolatile SRAM
Hardware information Serial number product Options and calibration Correction constants	N			
Temporary information storage for the CPU (CPU, cache and swap area)		N		
Operating system and instrument firmware			N	
Flash file system user defined antenna data			S	
User saved data sets				S

Table 4-2: The PC board for the GUI is equipped in R&S ESMD model 03

Data	PC EEPROM	PC SDRAM	PC Bios FLASH	PC Removable Compact-Flash™ Memory
Hardware information Serial number product Options and calibration Correction constants	N			
Temporary information storage for the CPU (CPU, cache and swap area)		N		
Basic I/O and settings			N	N
Operating system Restore (backup partition) Instrument firmware and help				N
Profiles (preset, startup)				S
Logging (errors and warnings)				N
Recording (audio and I / Q data)				S
Reports (test status)				N
Snapshot (screen shots)				S

N = No security concern

S = Security concern

5 Information Security in Highly Sensitive Areas

Since the SDRAM is erased when power is removed from the R&S ESMD it does not pose a security risk.

No user data is written to the EEPROMs, the processor board FLASH and the BIOS-FLASH memory; hence, it is deemed that it does not pose a risk either.

The processor board FLASH memory part containing the flash file system for antenna correction and antenna factor data can be accessed by the user via FTP (see also Correction_Data.pdf on the Firmware & Utilities CD). If this flash file system has been used for user antenna data this data can easily be deleted via FTP if they are a security concern.

The nonvolatile SRAM is a memory device that does not lose its memory when power is removed because it is buffered by the backup battery. This memory contains user data like receiver settings, memory channel list and suppress list. Therefore, this memory device must be cleared prior to leaving the secured area. (see chapter 6.1, "Memory Clearing Procedure", on page 12)

The PC Removable CompactFlash™ Memory does not lose its memory when power is removed and can contain user data. It can be removed from the R&S ESMD leaving the customer assured that no user data is stored within the wideband monitoring receiver.

The R&S ESMD equipped with the PC Removable CompactFlash™ Memory addresses the needs of customers working in highly sensitive areas.

6 Service, Calibration and Maintenance in Sensitive Areas

6.1 Memory Clearing Procedure

Master preset procedure to clear the nonvolatile SRAM

To remove any classified user data from the R&S ESMD perform the following steps:

syst:res:cold

SYSTem:RESet:COLD This remote command forces a cold reboot of the main processor. Device parameters are set to factory settings. All communication interfaces are closed.

or

Reset

A reset is carried out when line "EXT_RST" (pin 16 of connector X11A) at the rear panel is briefly grounded (for example, via pin 17 of connector X11A) while the receiver is on. The data for the configuration of the LAN interface is stored in an EEPROM. It is not affected by power failures and cannot be changed by a reset.

Factory setting procedure via GUI

PRESET: DEFAULT puts the R&S ESMD into the default state.

Suppress List Setup Dialog. Clear all deletes the suppress list.

Memory List Setup Dialog. Clear all deletes the memory channel list.

6.2 Removing the CompactFlash™ Memory

R&S ESMD equipped with the removable CompactFlash™ Memory

Remove the classified CompactFlash™ Memory (with the user data). This cannot be done without opening the wideband monitoring receiver.

To remove the hard drive, perform the following steps:

6.2.1 Disassembling the R&S ESMD

DANGER

Shock hazard

For all disassembly and reassembly work, ensure that the R&S ESMD is switched off and disconnected from the power supply by removing the plug from the AC and DC power connector, respectively.

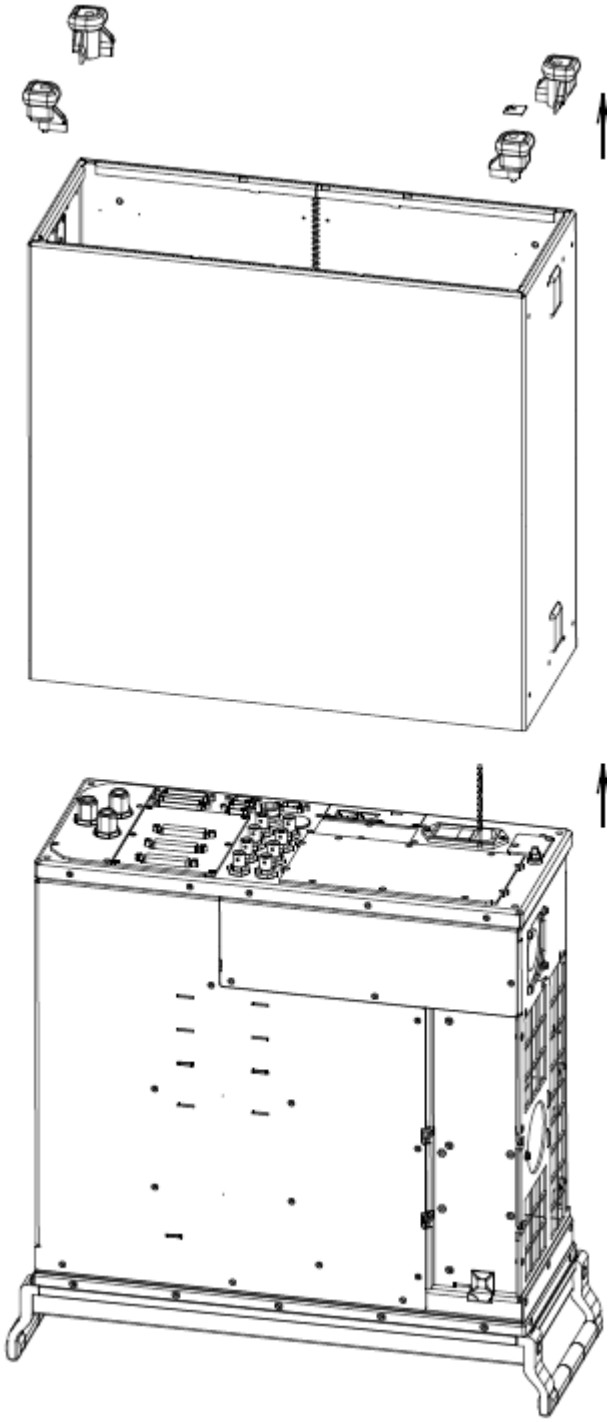

Fig. 6-1: Disassembly of the R&S ESMD.

- Switch off the R&S ESMD and unplug the power cable.
- Remove the cabinet feet (four recessed screws, size 2).
- Place the R&S ESMD on handles at the front.
- Push the casing upwards and remove it.

6.2.2 Installing a Compact Flash (CF) Card

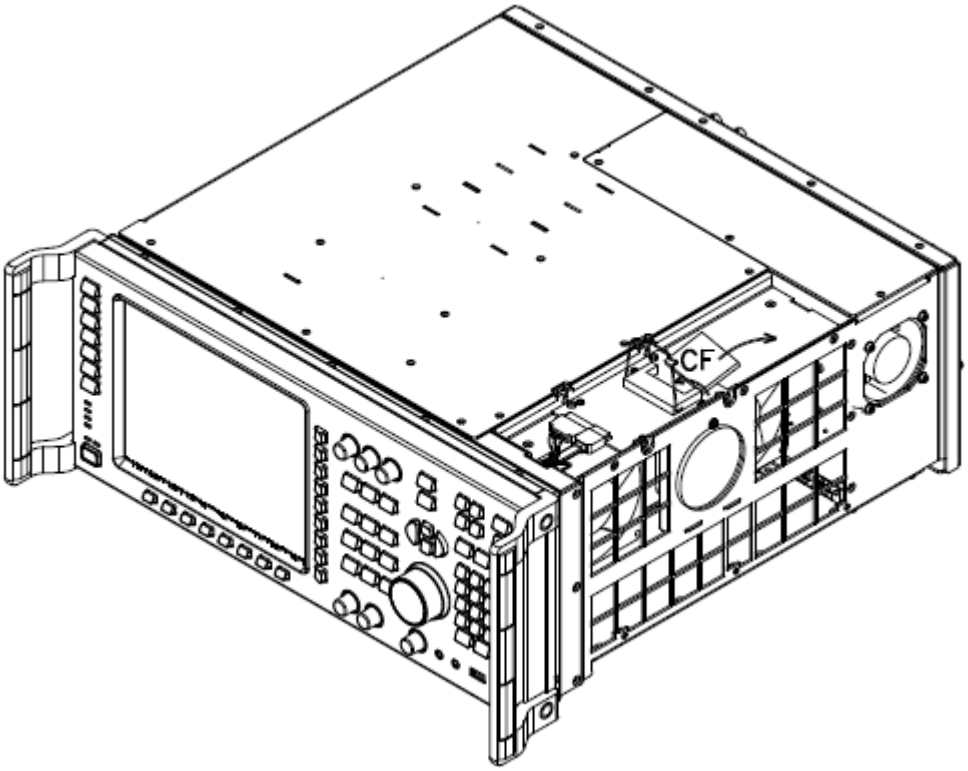

Fig. 6-2: Installing a CF card.

- Open the CF card holder.
- Remove the CF card.
- Plug in a new CF card.
- Close the CF card holder.

After installation of the new CF card you have to recover the image from the recovery CD.

6.3 Calibration

Clearing the nonvolatile SRAM or removing the CompactFlash™ Memory has no influence on the validity of calibration data.

7 Firmware Updates and Backing-Up User Data in Sensitive Areas

Rohde & Schwarz highly recommends, but does not require, the users of its products to maintain their products with the latest updates and to regularly back-up important user data that can be erased. Firmware updates are available from the R&S website.

There are several options available for the user to safely perform these operations without compromising the security of the sensitive areas.

7.1 Firmware Update via the LAN Interface

The R&S ESMD is equipped with a LAN interface as standard equipment. A user can transport the firmware update into the secure area via a CD or another medium that meets the security requirements. The update can then be placed on a system on the LAN within the secure area. The R&S ESMD can be updated directly from the LAN. The LAN can likewise be used to backup user data to an approved storage medium.

7.2 GUI Firmware Update via the USB port

The R&S ESMD model 03 is equipped with USB ports as standard equipment. The instrument firmware update can be performed directly from the USB stick. The USB stick can likewise hold or transport user data back-ups to an approved storage medium. As described below, users can disable the capability of the USB ports for saving data (set to "read only"). For users that have not elected to disable the USB ports for writing data a memory stick can be used for backing-up user data.

8 Special Considerations for USB Ports

USB ports can pose a security threat in high-security locations. Generally, this threat comes from small USB pen drives (a.k.a. memory sticks, key drives, etc) which can be very easily concealed, yet can quickly read/write several GBytes of data.

Disable USB ports for writing user data.

The R&S ESMD can be updated with a utility to disable the write capability on any USB port for storage devices. This utility is available free of charge on the Rohde & Schwarz web site in the R&S ESMD download area or on the R&S ESMD Fimrware and Utilities CD. To disable the write capability copy the utility software to the R&S ESMD and run it once. After reboot the write capability on any USB memory device is disabled.