R&S®NRP
USB and LAN Power Sensors
Instrument Security Procedures

1177510402

ROHDE&SCHWARZ

Instrument Security Procedures

Version 04

Contents

1 Overview 2

2 Instrument Models Covered 2

3 Security Terms and Definitions 4

4 Types of Memory and Information Storage in the R&S Power Sensors 5

5 Secure Erase Procedures 7

6 Instrument Declassification 8

1 Overview

It is often imperative that R&S NRPxxN power sensors are used in a secured environment. Generally these highly secured environments do not allow any test equipment to leave the area unless it can be proven that no user information leaves with the test equipment. Security concerns can arise when devices need to leave a secured area, e.g. to be calibrated or serviced.

This document describes the types of memory and their usage in the R&S NRPxxN. It provides a statement regarding the volatility of all memory types and specifies the steps required to declassify an instrument through memory clearing or sanitization procedures. These sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS).

2 Instrument Models Covered

Product name	Order number
R&S®NRPxxS(N)	
R&S®NRP8S	1419.0006.02
R&S®NRP8SN	1419.0012.02
R&S®NRP18S	1419.0029.02
R&S®NRP18SN	1419.0035.02
R&S®NRP18S-10	1424.6721.02
R&S®NRP18S-20	1424.6738.02

Product name	Order number
R&S®NRP18S-25	1424.6744.02
R&S®NRP33S	1419.0064.02
R&S®NRP33SN	1419.0070.02
R&S®NRP33SN-V	1419.0129.02
R&S®NRP40S	1419.0041.02
R&S®NRP40SN	1419.0058.02
R&S®NRP50S	1419.0087.02
R&S®NRP50SN	1419.0093.02
R&S®NRPxxA(N)	
R&S®NRP6A	1424.6796.02
R&S®NRP6AN	1424.6809.02
R&S®NRP18A	1424.6815.02
R&S®NRP18AN	1424.6821.02
R&S®NRPxxT(N)	
R&S®NRP18T	1424.6115.02
R&S®NRP18TN	1424.6121.02
R&S®NRP33T	1424.6138.02
R&S®NRP33TN	1424.6144.02
R&S®NRP40T	1424.6150.02
R&S®NRP40TN	1424.6167.02
R&S®NRP50T	1424.6173.02
R&S®NRP50TN	1424.6180.02
R&S®NRP67T	1424.6196.02
R&S®NRP67TN	1424.6209.02
R&S®NRP110T	1424.6215.02
R&S®NRPxxTWG	
R&S®NRP75TWG	1700.2529.02
R&S®NRP90TWG	1700.2312.02
R&S®NRP110TWG	1173.8709.02

3 Security Terms and Definitions

Clearing

The term "clearing" is defined in Section 8-301a of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Clearing is the process of eradicating the data on media so that the data can no longer be retrieved using the standard interfaces on the instrument. Therefore, clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization

The term "sanitization" is defined in Section 8-301b of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned for service of calibration.

The memory sanitization procedures described in this document are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the "Clearing and Sanitization Matrix" in Section 14.1.16 of the ISFO "Manual for the Certification and Accreditation of Classified Systems under the NISPOM".

Instrument declassification

The term "instrument declassification" refers to procedures that must be undertaken before an instrument can be removed from a secure environment, for example when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. The declassification procedures described in this document are designed to meet the requirements specified in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", Chapter 8.

4 Types of Memory and Information Storage in the R&S Power Sensors

The R&S power sensors contain two independent processor systems; one is running the firmware application (MAIN) and the second one acts as a communication frontend for the USB channels (COMM). Both processor systems access various memory areas.

The following table provides an overview of the memory components that are part of your instrument. For a detailed description regarding type, size, usage and location, refer to the subsequent sections.

Memory type	Size	Content	Volatility	User data	Sanitization procedure
SDRAM MAIN processor	512 MiB	RAM used by operating system, firmware and FPGA to control the power sensor operation	Volatile	Yes	Turn off instrument power (disconnect USB / LAN)
OCRAM MAIN processor	256 KiB	On-chip RAM of processor; used for booting the sensor only	Volatile	No	Turn off instrument power (disconnect USB / LAN)
SRAM COMM processor	52 KiB	Communication and interface protocols (USB)	Volatile	Yes	Turn off instrument power (disconnect USB / LAN)
Flash COMM processor	256 KiB	Firmware for communication channels (USB) of the sensor	Non-volatile	No	None required
Flash MAIN processor	64 MiB	Boot code, operating system and sensor firmware; user data (user calibration data, save/recall settings, configuration settings)	Non-volatile	Yes	Secure erase (see Chapter 5, "Secure Erase Procedures", on page 7)

4.1 Volatile Memory

The volatile memory in the instrument does not have battery backup. It loses its contents as soon as power is removed from the instrument (disconnect USB or LAN). The volatile memory is not a security concern.

Removing power from this memory meets the memory sanitization requirements specified in the "Clearing and Sanitization Matrix" in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

SDRAM (MAIN processor)

The SDRAM has a size of 512 MiB SDRAM.

It is used by the operating system, the firmware and FPGA to control the power sensor functionality.

Sanitization procedure: Turn off instrument power (disconnect USB or LAN)

OCRAM (MAIN processor)

The OCRAM has a size of 256 KiB.

It is used to boot the power sensor.

Sanitization procedure: Turn off instrument power (disconnect USB or LAN)

SRAM

The SRAM has a size of 52 KiB.

It is used by the COMM processor for the communication and interface protocols.

Sanitization procedure: Turn off instrument power (disconnect USB or LAN)

4.2 Non-Volatile Memory

The R&S power sensors contain non-volatile memory on both processor systems, MAIN and COMM.

Flash (COMM processor)

The flash memory on the COMM processor has a size of 256 KiB.

It contains the COMM processor firmware. The firmware controls the communication channels (USB) of the power sensor.

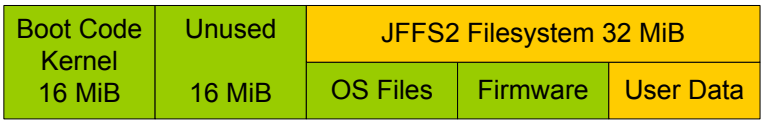
In addition, it contains sensor specific data. The memory is programmed in the factory or through firmware updates in the field.

The flash memory on the COMM processor does not hold user data nor can the user access the microcontroller flash memory.

Sanitization procedure: None required (no user data)

Flash (MAIN processor)

The serial NOR flash memory has a size of 64 MiB. It is partitioned in different sections.



- Boot code kernel
  This section has a size of 16 MiB and contains boot code (u-boot images) and the operating system kernel.
  This section is initialized during production and during firmware updates. It cannot be accessed by the user and is not modified during instrument operation.
- Unused section
  This section has a size of 16 MiB and is currently unused and reserved for later use.
  This section cannot be accessed by the user and is not modified during instrument operation.
- JFFS2 file system
  This section has a size of 32 MiB and is controlled by the JFFS2 file system (Journaling Flash File System).
  It contains the main firmware and user data.
  The main firmware includes the root file system, measurement firmware including factory calibration data and web pages.
  User data includes user calibration data, save/recall data, configuration settings.

Sanitization procedure: Secure Erase

with remote I/O command: `SERVice:SECure:ERASe`, see next chapter for details.

5 Secure Erase Procedures

Because the SDRAM, the OCRAM and the SRAM are erased when power is removed from the power sensor, they do not pose a security risk. The flash memory on the COMM processor contains no user data. Therefore, it is deemed that it does not pose a risk either.

The flash memory on the MAIN processor is the only memory type that does not lose its contents when power is removed. It can contain user data.

You can sanitize the flash memory by sending the remote I/O command `SERVice:SECure:ERASe` to the power sensor.

`SERVice:SECure:ERASe` triggers the following actions:

- Operating system files and power sensor firmware are temporarily saved.
- A full sector erase command as per manufacturer data sheet is applied to every single sector of the JFFS2 area.
- Every addressable location of the JFFS2 area is overwritten by a single character.

- Another full sector erase command as per manufacturer data sheet is applied to every single sector of the JFFS2 area.
- The JFFS2 file system is recreated and operating system files as well as instrument firmware are restored.

The Secure Erase Procedure meets the memory sanitization requirements specified in the "Clearing and Sanitization Matrix" in Section 14.1.16 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

6 Instrument Declassification

Before you can remove the power sensor from a secured area (for example to perform service or calibration), all classified user data needs to be removed. You can declassify the power sensor as follows:

1. Connect the power sensor via USB or LAN to a PC.
2. Sanitize the non-volatile memory as described in Secure Erase Procedures by sending the remote I/O command sequence:
   `SERVice:UNLock 1234` // enables service functions
   `SERVice:SECure:ERASe`

   The sanitization will last approximately 10 minutes. During that time, the white LED on the power sensor blinks with a rate of 1.5 sec. After completion, you can query the result with the remote I/O command:
   `SERVice:UNLock 1234`
   `SERVice:SECure:ERASe:STATus?`
   which will return the number of sanitization cycles so far, and the status/error information of the last sanitization, e.g. `"Conter:2","Error:none"`. Typically you will read out this information before starting the sanitization, keep the counter in mind, and check after sanitization that the counter is 1 higher than before.
3. After memory sanitization, disconnect the power sensor from USB or LAN to remove power supply.

R&S NRP Sanitizer tool

Another alternative to directly sending the sanitization command to the power sensor (as described in step 2), is to use the R&S NRP Sanitizer tool which is available from the Internet site, see www.rohde-schwarz.com.

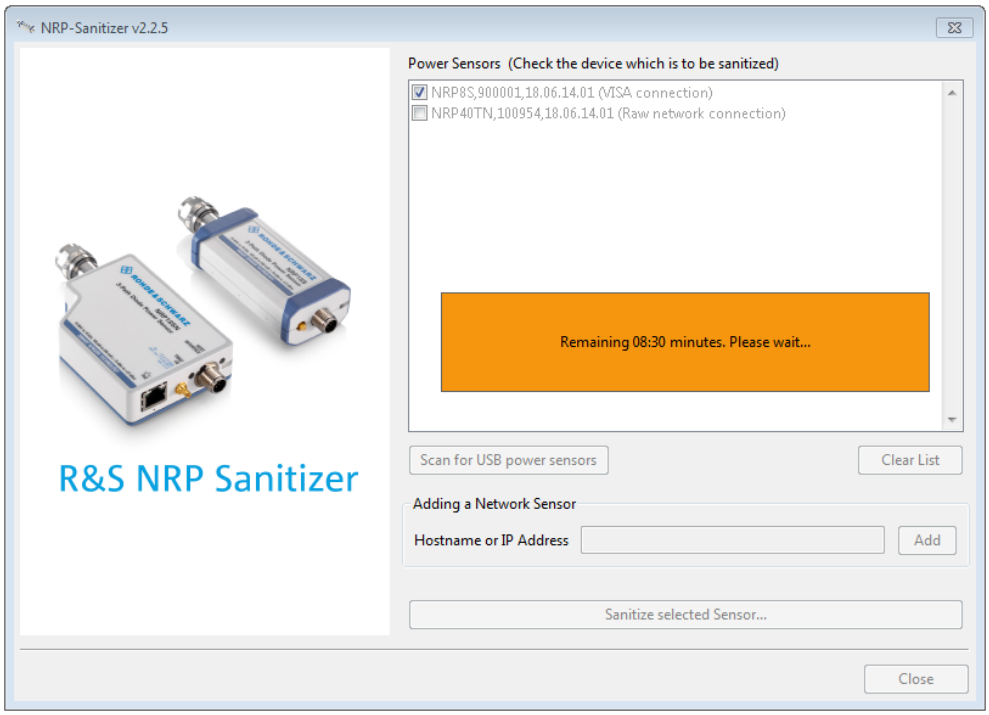
This tool requires Microsoft®Windows 7 or Microsoft®Windows 10 and an installed VISA library.

After downloading the installer file to your PC and installing the R&S NRP Sanitizer perform the following steps:

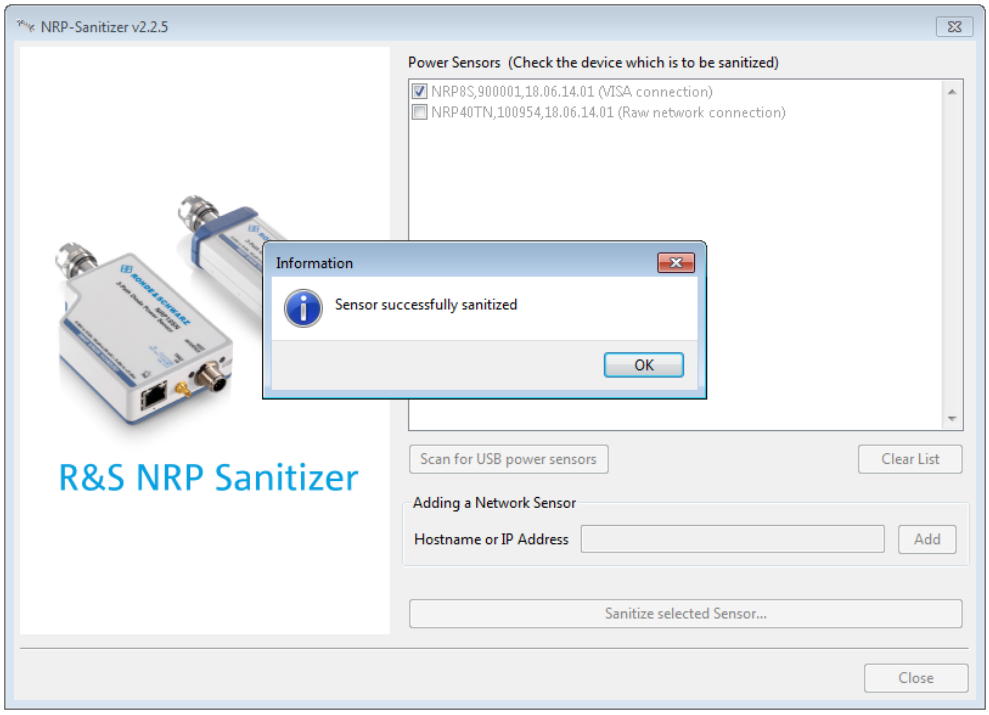
1. Start the tool.

The R&S NRP Sanitizer tool scans automatically for USB power sensors. For LAN power sensors, enter the corresponding address information in the "Hostname or IP Address " field to add the sensor to the list.

2. Select the R&S power sensors you need to sanitize from the list of connected power sensors.
3. Start the sanitizing.



4. After the sanitization process is complete, the following message is displayed on the screen:



5. Finally disconnect the R&S power sensors from USB or LAN to remove power supply.

Following these steps removes all user data from the power sensor. The power sensor can now leave the secured area.

These declassification procedures meet the needs of customers working in secured areas.

Validity of instrument calibration after declassification

During the declassification procedure, the power sensor factory calibration data is saved and later restored to allow for sensor recalibration. The power sensor remains fully functional after declassification.

In certain cases, for example if the sensor has no saved factory calibration data, the complete user data including the calibration data is being erased from the sensor.

In this case, the sensor will come up with a red blinking LED in "Fail-Safe-Mode". For recalibration it is necessary to contact the Rohde & Schwarz Backup Service to get the factory calibration data of the sensor.

After the calibration data are written to the sensor, it is fully functional for recalibration.

Mühldorfstr. 15, 81671 München, Germany
Phone: +49 89 41 29 - 0
Fax: +49 89 41 29 12 164
Email: info@rohde-schwarz.com
Internet: www.rohde-schwarz.com