R&S®NRP Power Sensors / R&S®NRQ6 / R&S®NRPM3 Instrument Security Procedures

ROHDE&SCHWARZ

Make ideas real

This document describes the types of memory and their usage of the R&S®NRP power sensors, R&S®NRQ6 power sensors and the R&S®NRPM3 power sensor modules.

Throughout this manual, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®NRP18SN is indicated as R&S NRP18SN. An R&S NRP power sensor or power sensor module is also referred to as instrument.

Contents

1 Overview

Securing important information is crucial in many applications.

Generally, 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, e.g. to be calibrated.

"Regarding sanitization, the principal concern is ensuring that data is not unintentionally released" [1].

This document provides a statement regarding the volatility of the memory types used and specifies the steps required to sanitize an instrument.

The procedures in this document follow "NIST Special Publication 800-88: Guidelines for Media Sanitization" [1].

In addition, recommendations are provided to safeguard information on the product.

References

See the following literature for further information.

[1]   **Kissel Richard L. [et al.]** Guidelines for Media Sanitization = Special Publication (NIST SP) = NIST SP - 800-88 Rev 1. - Gaithersburg : [s.n.], December 17, 2014.

[2]   **National Industrial Security Program Authorization Office** Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM). - May 6, 2019.

[3]   **ACSC Australian Cyber Security Centre** Australian Government Information Security Manual, January 2020.

2 Instrument models covered

Table 2-1: R&S NRP power sensor / R&S NRQ6 / NRPM3(N) models

Product name	Order number
R&S NRPxxS(N)	
R&S NRP8S	1419.0006K02
R&S NRP8SN	1419.0012K02
R&S NRP18S	1419.0029K02
R&S NRP18SN	1419.0035K02
R&S NRP18S-10	1424.6721K02
R&S NRP18S-20	1424.6738K02
R&S NRP18S-25	1424.6744K02
R&S NRP33S	1419.0064K02
R&S NRP33SN	1419.0070K02
R&S NRP33SN-V	1419.0129K02
R&S NRP40S	1419.0041K02
R&S NRP40SN	1419.0058K02
R&S NRP50S	1419.0087K02
R&S NRP50SN	1419.0093K02
R&S NRP67S	1424.6396K02
R&S NRP67SN	1424.6409K02
R&S NRP67SN-V	1424.6415K02
R&S NRP90S	1424.6421K02 1424.6421K03
R&S NRP90SN	1424.6450K02
R&S NRPxxA(N)	
R&S NRP6A	1424.6796K02
R&S NRP6AN	1424.6809K02
R&S NRP18A	1424.6815K02
R&S NRP18AN	1424.6821K02
R&S NRPxxT(N)	
R&S NRP18T	1424.6115K02
R&S NRP18TN	1424.6121K02
R&S NRP33T	1424.6138K02

Product name	Order number
R&S NRP33TN	1424.6144K02
R&S NRP40T	1424.6150K02
R&S NRP40TN	1424.6167K02
R&S NRP50T	1424.6173K02
R&S NRP50TN	1424.6180K02
R&S NRP67T	1424.6196K02
R&S NRP67TN	1424.6209K02
R&S NRP90T	1424.6473K02
R&S NRP90TN	1424.6480K02
R&S NRP110T	1424.6215K02
R&S NRPxxTWG(N)	
R&S NRP75TWG	1700.2529K02
R&S NRP75TWGN	1440.5010K02
R&S NRP90TWG	1700.2312K02
R&S NRP90TWGN	1440.5078K02
R&S NRP110TWG	1173.8709K02
R&S NRP110TWGN	1440.5132K02
R&S NRPxxP	
R&S NRP18P	1444.1190K02
R&S NRP40P	1444.1290K02
R&S NRP50P	1444.1390K02
R&S NRQ6	
R&S NRQ6	1421.3509K02
NRPM3N	
R&S NRPM3	1425.8563.02
R&S NRPM3N	1425.8592.02

3 Security terms and definitions

Terms defined in Guidelines for Media Sanitization

According to NIST Special Publication 800-88 [1]: "Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort." It defines the following categories of sanitization:

- **"Sanitization"**
  "Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort."
- **"Clear"**
  "Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported)."
- **"Purge"**
  "Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques."
- **"Destroy"**
  "Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data."

Control of media

Another option to secure sensitive information is to keep physical media within the classified area, see [1], paragraph 4.4.

Volatile memory

"Memory components that do not retain data after removal of all electrical power sources, and when reinserted into a similarly configured system, are considered volatile memory components." [2]

Typical examples are RAM, e.g. SDRAM.

Non-volatile memory

"Components that retain data when all power sources are discontinued are non-volatile memory components." [2].

In the context of this document, non-volatile memory components are non-user accessible internal memory types, e.g. EEPROM, Flash, etc.

Media

Media are types of non-volatile memory components. In the context of this document, media are user-accessible and retain data when you turn off power.

Media types are Hard Disk Drives (HDD), Solid State Drives (SSD), Memory Cards, e.g. SD, microSD, CFast, etc., USB removable media, e.g. Pen Drives, Memory Sticks, Thumb Drives, etc. and similar technologies.

4 Statement of volatility

The Rohde & Schwarz power sensors/power sensor modules contain various memory components. See the subsequent sections for a detailed description regarding type, size, usage and location.

ⓘ **Notes on memory sizes**

Due to the continuous development of memory components, the listed values of memory sizes may not represent the current, but the minimal configuration.

This document uses the common notation kbyte, Mbyte and Gbyte for memory sizes, although the prefix multiplication factor is 1024.

4.1 Volatile memory

Volatile memory modules refer to non-accessible internal storage devices, as described in Security terms and definitions > Volatile memory.

Table 4-1: Types of volatile memory

Memory type	Location	Size	Content / Function	User modifiable
R&S NRPxxA(N) / R&S NRPxxS(N) / R&S NRPxxT(N) / R&S NRPxxTWG(N) / R&S NRP18S-xx / NRPM3(N)				
OCRAM	Main processor	256 kbyte	Boot code	No
Block RAM	Main processor, FPGA	0.5 Mbyte	Control of power sensor operation	Yes
SDRAM		512 Mbyte	• Operating system • Firmware	Yes
SRAM	COMM processor	52 kbyte	Communication and interface protocols (USB)	Yes
R&S NRPxxP				
SRAM	Microcontroller	524 kbyte	Firmware	No
		548 kbyte	not used	No
Block RAM	Main processor, FPGA	1296 kbit	Control of power sensor operation	No
SDRAM		64 Mbyte	Static data structures	No
R&S NRQ6				
OCRAM	Main processor	256 kbyte	Boot code	No
Block RAM	Main processor, FPGA	2 Mbyte	Control of power sensor operation	Yes
SDRAM		512 Mbyte	• Operating system • Firmware	Yes
RAM	PLD	8 kbyte	Internal memory for peripherals control	Yes
SRAM	COMM processor	52 kbyte	Communication and interface protocols (USB)	Yes

4.2 Non-volatile memory

Non-volatile memory modules refer to non-accessible internal storage devices, as described in Security terms and definitions > Non-volatile memory.

Table 4-2: Types of non-volatile memory

Memory type	Location	Size	Content / Function	User modifiable
R&S NRPxxA(N) / R&S NRPxxS(N) / R&S NRPxxT(N) / R&S NRPxxTWG(N) / R&S NRP18S-xx / NRPM3(N)				
Flash		16 Mbyte	• Bootloader • FPGA configuration • OS Kernel	No
		16 Mbyte	Temporary storage for firmware during sanitization	No
		32 Mbyte	JFFS2 file system: • Operating system • Main application • Calibration data • Instrument settings • Product options	Yes
Flash	COMM processor	256 kbyte	• Firmware for communication channels (USB) • Sensor-specific data	No
R&S NRPxxP				
Flash	Microcontroller	2 Mbyte	Application firmware	No
Flash	CPU board	32 MByte	• Target descriptor (device ID) • FPGA configurations • Factory calibration data	No
			• User calibration data • Instrument settings	Yes
R&S NRQ6				
Flash		32 Mbyte	• Bootloader • FPGA configuration • OS Kernel	No
		32 Mbyte	Temporary storage for firmware during sanitization	No
		64 Mbyte	JFFS2 file system: • Operating system • Main application • Calibration data • Instrument settings • Product options	Yes
Flash	PLD	42 kbyte	Firmware for peripherals control	No
Flash	COMM processor	256 kbyte	• Firmware for communication channels (USB) • Sensor-specific data	No

4.3 Media

The Rohde & Schwarz power sensors/power sensor modules do not contain media, as defined in Security terms and definitions > Media.

5 Instrument sanitization procedure

Considerations on the sanitization procedure

- Maintaining operability
  Make sure that the instrument remains power supplied and switched on during sanitization. Turning off or disconnecting the instrument from the mains while the sanitization procedure is running results in loss of calibration data.
  Thus, the functionality of the product is no longer ensured.

- About the sanitization procedure

  To clear the non-volatile memory, the sanitization process executes several steps that affect the product-specific memory partitions:

  – Except for R&S NRPxxP power sensors, see Sanitization process of the product.

  – For R&S NRPxxP power sensors, see "Sanitization process of the R&S NRPxxP power sensors" on page 14.

- Starting the sanitization procedure

  You have several options to start the sanitization procedure:

  – By I/O remote control commands, see Remote I/O

  – By the R&S power meter sanitization tool

- Security status after sanitization
  Sanitization clears all security settings. In particular, it resets all passwords to factory values.

5.1 Volatile memory

You can clear the volatile memory by following the procedure below. The sanitization procedure complies with the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 8.

To remove power from LAN power sensors/power sensor modules

A LAN power sensor/power sensor module can be powered over Ethernet (PoE), either by an Ethernet switch, or a PoE injector, but also powered by USB.

1. Disconnect the LAN connection cable.

2. Disconnect the USB connection cable.

   Leave the instrument powered off at least for 30 seconds to make sure that all volatile memory modules lose their contents, see [3].

To remove power from USB power sensors / power sensor modules

► Disconnect the USB connection cable.

Leave the instrument powered off at least for 30 seconds to make sure that all volatile memory modules lose their contents, see [3].

5.2 Non-volatile memory

You can clear the non-volatile memory by following the procedure below. The sanitization procedure complies with the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 8.

Sanitization process of the R&S NRPxxP power sensors

The sanitization procedure implemented for R&S NRPxxP power sensors executes the following actions:

1. Saves the instrument firmware (including the product options) temporarily.

2. Erases the flash pages (flash erase).

3. Overwrites each addressable location of the flash pages by 0x00 (binary zero) characters.

4. Erases the flash pages again.

5. Recreates the flash pages file system and restores the instrument firmware.

Sanitization process of the product

"Product" applies to all remaining power sensors/power sensor modules except for R&S NRPxxP power sensors.

The sanitization procedure implemented for the product executes the following actions:

1. Saves the instrument firmware (including the product options) temporarily.

2. Erases the JFFS2 partition partition (flash erase).

3. Overwrites each addressable location of the JFFS2 partition by 0x00 (binary zero) characters.

4. Erases the JFFS2 partition again.

5. Recreates the JFFS2 file system and restores the instrument firmware.

5.2.1 Remote I/O

To sanitize the non-volatile memory remotely

1. Connect the instrument to a controller device, either in a LAN or over USB.

2. Start a controller application program on the controller.

3. Before starting the sanitization procedure, we recommend that you read out the status of the last sanitization.
   Send the following commands:
   `SERVice:UNLock 1234`   // enables service functions
   `SERVice:SECure:ERASe:STATus?`
   Returns the number of the executed sanitization cycles so far, and the status/error information of the last sanitization, e.g. `"Counter:2","Error:none"`.
   Keep the counter in mind.

4. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
   Make sure that the instrument is continuously supplied with power as long as the process is running.
   NOTICE! The sanitization procedure clears all user data and resets the instrument.
   Send the following remote I/O command sequence to the instrument:
   `SERVice:UNLock 1234`
   `SERVice:SECure:ERASe`
   The procedure "Sanitize internal memory" starts. The application indicates the currently performed action and its progress.

5. When completed, you can query the result with the following command sequence:
   `SERVice:UNLock 1234`
   `SERVice:SECure:ERASe:STATus?`
   Check if the counter has incremented by 1 after sanitization, e.g. `"Counter:3","Error:none"`.

5.2.2 R&S power meter sanitization tool

As an alternative to sending the sanitization commands to the instrument (as described in Chapter 5.2.1, "Remote I/O", on page 14), you can use the R&S power meter sanitization tool which is provided on the Rohde & Schwarz website.

The R&S power meter sanitization tool must be installed on a controller PC and requires Microsoft®Windows 7, Microsoft®Windows 10 or Microsoft®Windows 11 operating system and an installed VISA library.

Rohde & Schwarz provides the VISA library free of charge for download on the Internet, see http://www.rohde-schwarz.com/rsvisa.

For detailed information, including download and installation of the application, see Chapter 8, "R&S power meter sanitization tool", on page 19

To sanitize the non-volatile memory with the R&S power meter sanitization tool

It is assumed, that you have installed the R&S power meter sanitization tool on the controller PC. Therefore, the following section briefly outlines the main steps to execute the procedure.

1. Start the R&S power meter sanitization tool.

   The application scans automatically for instruments connected over USB. For instruments connected in the LAN, enter the corresponding address information to add the instrument to the list.

2. Select the instrument from the list.

3. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
   Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   Start the sanitization procedure.

   The R&S power meter sanitization tool confirms with a message when completed.

5.3 Media

The product does not contain media memory modules. Therefore no sanitization procedure is required.

6 Operability outside secured area

The sanitization procedure saves the firmware temporarily and restores it for recreation, see the description of the sanitization steps in Chapter 5.2, "Non-volatile memory", on page 14.

Thus the operability of the instrument is maintained after sanitization.

7 Validity of instrument calibration

The validity of the instrument's calibration is maintained throughout the sanitization.

► **NOTICE!** If the instrument has been powered off during the sanitization procedure, the calibration data is lost.

Contact the Rohde & Schwarz backup service to get the factory calibration data for recalibration of the instrument.

8 R&S power meter sanitization tool

R&S power meter sanitization tool is a PC application that helps you to declassify a Rohde & Schwarz instrument before it leaves a secure environment. The application executes a procedure that removes all user data from the instrument.

This declassification procedure meets the needs of customers working in a secured area.

Instruments covered

You can use the R&S power meter sanitization tool to sanitize the following instruments:

- R&S NRX / R&S NRT2 power meters
- R&S NRP power sensors
- R&S NRQ6 power sensors
- NRPM3(N) power sensor modules
- R&S NRPCxx(-B1) / R&S NRPC-LS power sensor calibration kits

8.1 Setting up the R&S power meter sanitization tool

Prerequisites

The R&S power meter sanitization tool runs on PCs with Microsoft®Windows 7, Microsoft®Windows 10 or Microsoft®Windows 11 operating system with an installed VISA library.

Rohde & Schwarz provides the VISA library free of charge for download on the Internet, see http://www.rohde-schwarz.com/rsvisa.

The R&S power meter sanitization tool is available free of charge also. You can download the program file `NrpSanitizer_Installer_x.x.xxxx.xxxx.exe`[1] from the product page of any of the supported instruments, e.g. www.rohde-schwarz.com/software/nrp

[1] xx represents the current version of the application.

The installer program contains all components required for installation and operation of the R&S power meter sanitization tool.

To install the application

1. Download the latest version of the R&S power meter sanitization tool installer program.

2. Execute `NrpSanitizer_Installer_x.x.xxxx.xxxx.exe` and follow the instructions of the installation wizard.

   The setup program checks if a VISA library is available and installs the application files.
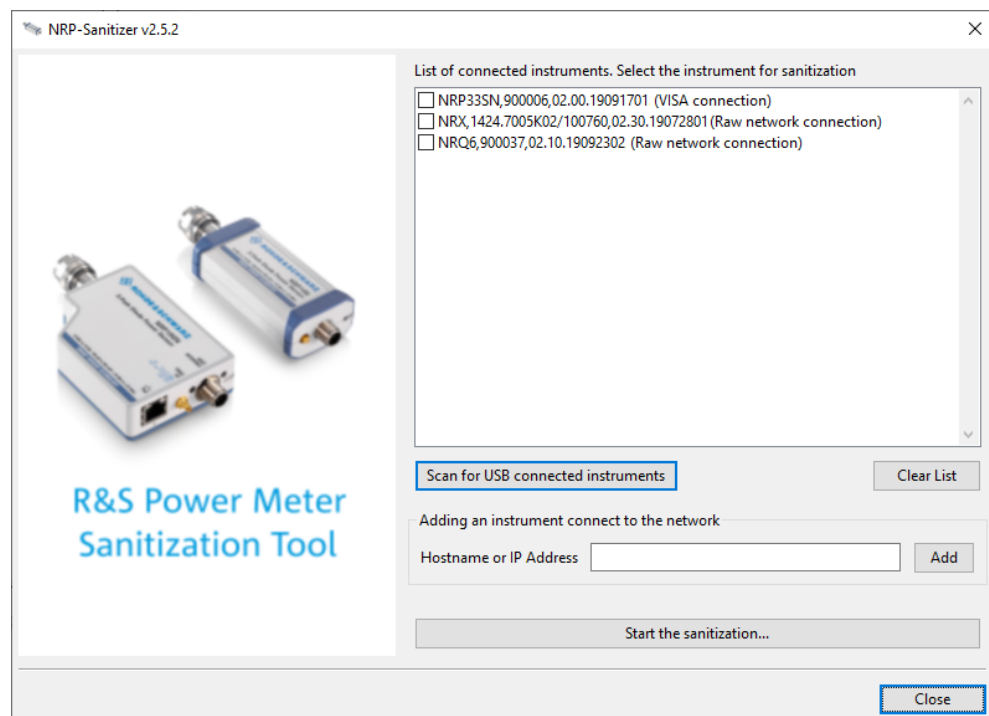
8.2 Starting the sanitization

After downloading the installer file to your PC and installing the R&S power meter sanitization tool, perform the following steps:
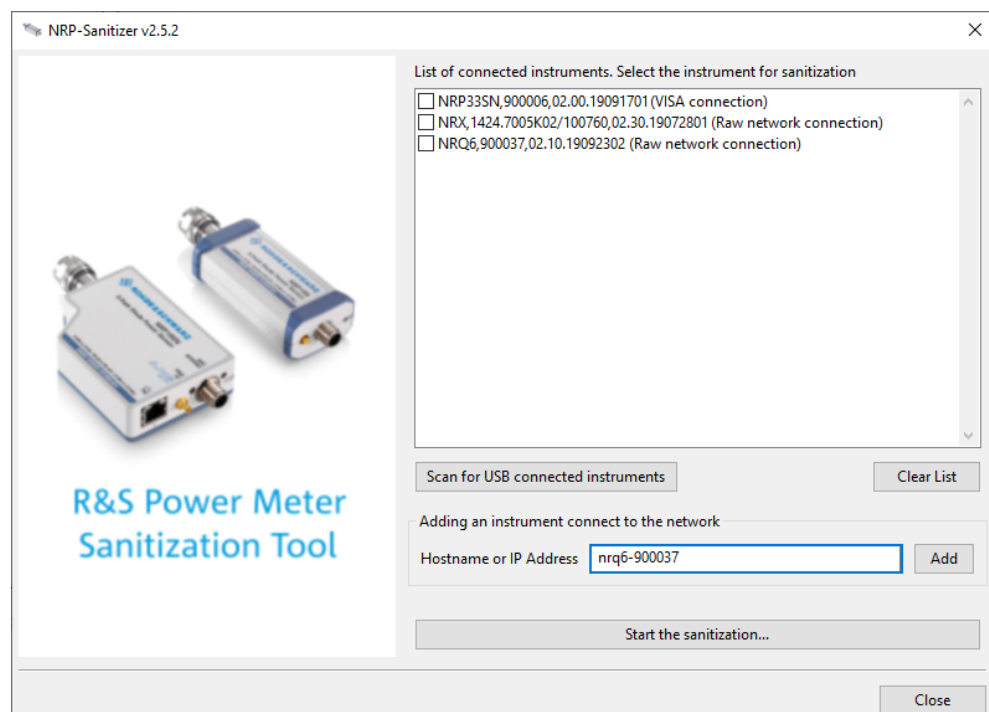
1. Start the application.
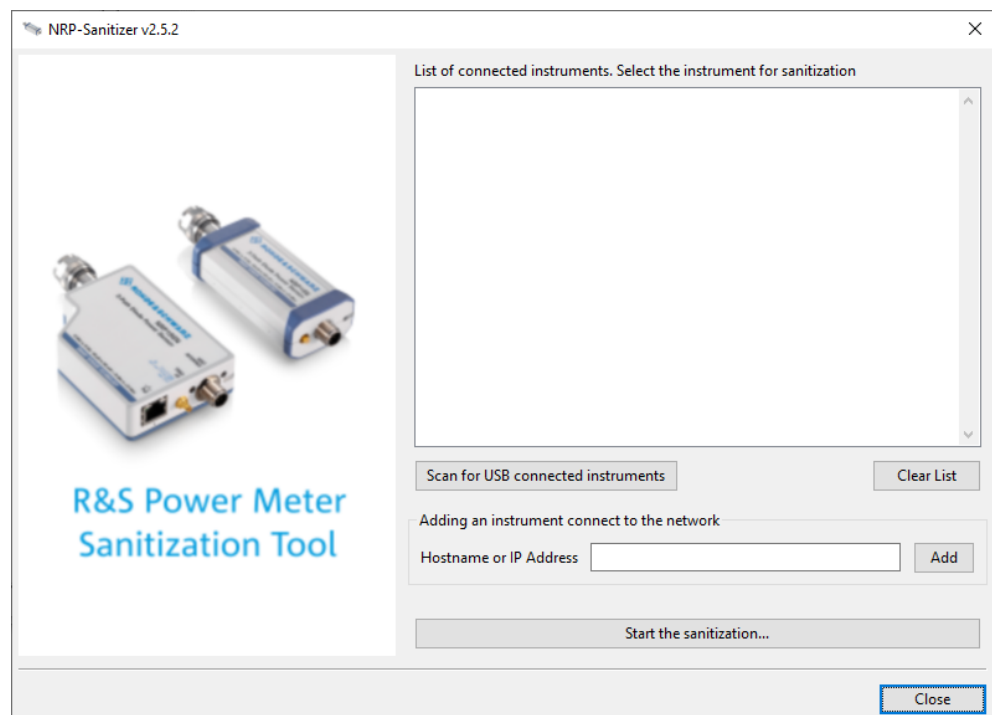
2. To search for USB connected instruments, select "Scan for USB connected instruments".

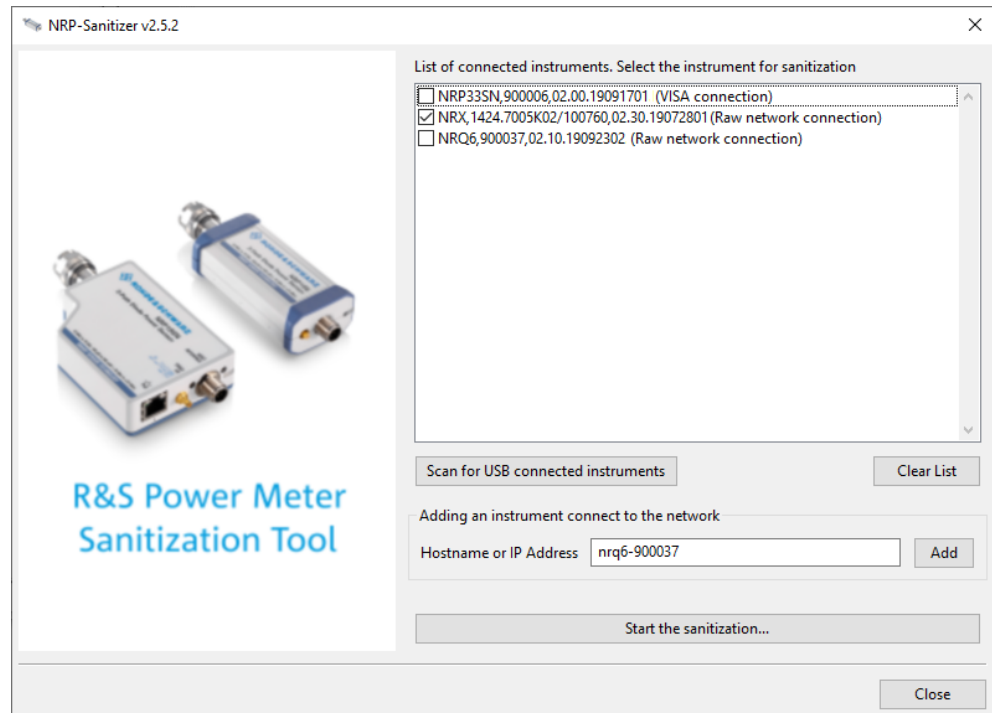The application lists all supported instruments connected to the USB interfaces.

3. For instruments connected to the LAN, enter the corresponding address information in the "Hostname or IP Address" field.


4. Confirm with "Add".

The application adds the instrument to the list.

5. Select the instrument you need to sanitize from the list.

6. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   "Start the sanitization..." and confirm the execution.
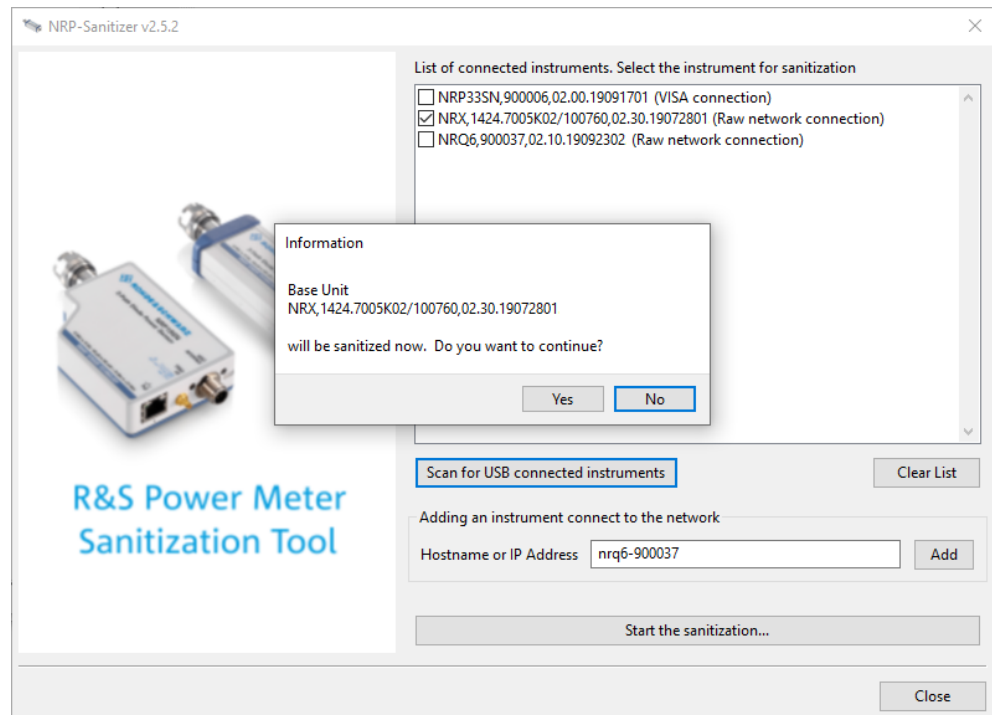
The sanitization lasts approximately 10 minutes.
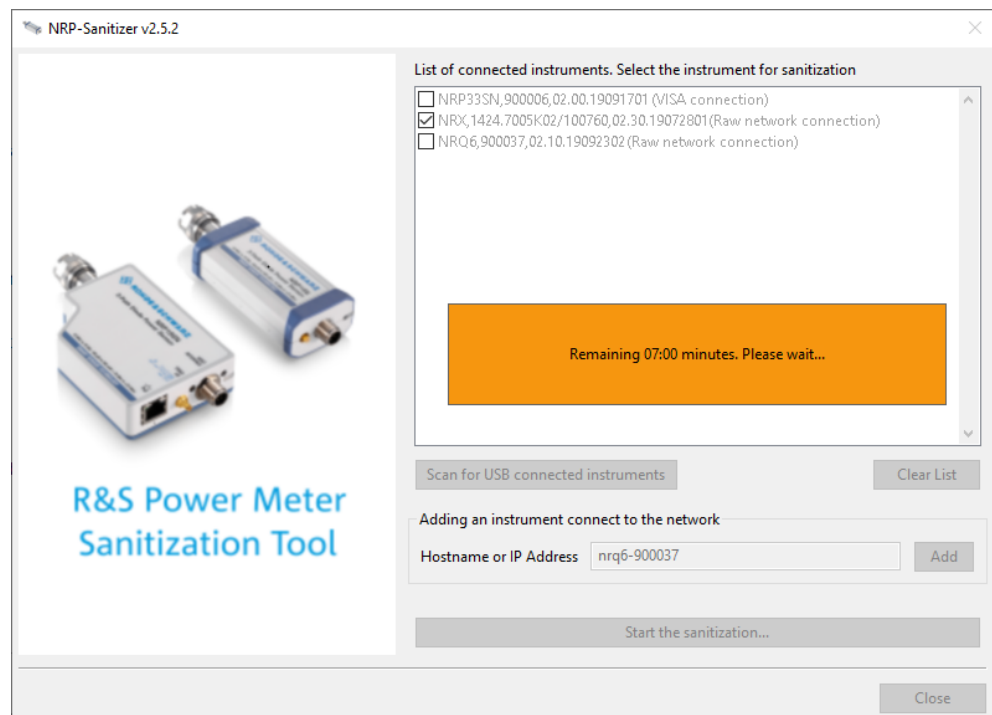
7. The R&S power meter sanitization tool also validates the sanitization and confirms with a message when completed.