Declassification of the InfiniiVision HD3-Series Oscilloscopes

KEYSIGHT

USER'S GUIDE

Notices

Manual Part Number

54760-97005

Edition

First edition, September 2024

Available in electronic format only

Published by:
Keysight Technologies, Inc.
1900 Garden of the Gods Road
Colorado Springs, CO 80907 USA

Print History

54760-97005, June 2024

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology License

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Contents

1 Declassification and Security

This document describes instrument security features and the steps to declassify an instrument through memory clearing, sanitization, or removal.

For additional information, go to:

http://www.keysight.com/find/security

NOTE

Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Keysight Technologies cannot be held responsible for any lost files or data resulting from the clearing of memory. Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

Contacting Keysight Sales and Service Offices

Assistance with test and measurement needs, and information on finding a local Keysight office, is available on the Internet at:

http://www.keysight.com/find/assist

If you do not have access to the Internet, please contact your field engineer.

NOTE **In any correspondence or telephone conversation, refer to the instrument by its model number and full serial number. With this information, the Keysight representative can determine whether your unit is still within its warranty period.**

Products Covered by this Document

Table 1 InfiniiVision HD3-Series Oscilloscopes

Model number	Bandwidth	Sample rate	Memory	Analog channels	Digital channels
HD302MSO	200 MHz standard, options for 350 MHz, 500 MHz, and 1 GHz	3.2 GSa/s	20 Mpts standard, options for 50 Mpts and 100 Mpts	2	16
HD304MSO		3.2 GSa/s		4	16
Product family name: HD-Series Oscilloscope Product name: InfiniiVision HD3-Series Oscilloscope Alternate product numbers: N/A					

Security Terms and Definitions

Term	Definition
Clearing	Clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.
Instrument Declassification	A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment, such as is the case when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both.
Sanitization	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 to the factory for calibration.
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

Instrument Memory

This section contains information on the types of memory available in your instrument. It explains the size of memory, how it is used, its location, volatility, and the sanitization procedure.

Table 2 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	Sanitization procedure
Acquisition / display memory, analog channels, 4 x up to 100 Mbytes (4 channel)	Yes	No	Scope channel acquisition / display memory for analog channels	Input signal data (ADC output)	System ASIC(s) and 16 Gb DRAMs (4 parts on board)	Cycle power
Acquisition / display memory, digital channels, 20 Mbytes (16 channels)	Yes	No	Scope channel acquisition / display memory for digital channels	Input signal data (digital channel inputs)	System ASIC(s) and 16 Gb DRAMs (4 parts on board)	Cycle power
Display memory (in 16 Gb DRAMs)	Yes	No	Display / screen memory	ASIC output	16 Gb DRAMs	Cycle power
P700 CPU ram 4 GB LPDDR4 DRAM	Yes	No	CPU system variables	Operating system	P700 card - 4 GB LPDDR4	Cycle power
P700 CPU system memory 16 GB eMMC	No	Yes	Bootloader, OS kernel, run-time libraries, InfiniiVision application	Factory Installed operating system	P700 card	No user data is stored
	No - written only during license upgrades	Yes	Licenses	Updated with purchase	P700 card	No user data is stored
	No - written only during calibration	Yes	Calibration	Calibration	P700 card	No user data is stored
	Yes	Yes	Internal customer storage	Normal operation	P700 card	**Secure Erase** or **Factory Reset**

Table 2 Instrument Memory (continued)

Memory type and size	Writable during normal operation?	Data retained when powered off?	Purpose/ contents	Data input method	Location in instrument and remarks	Sanitization procedure
FPGA program memory Serial NOR flash 32 Mbytes	No	Yes	FPGA firmware loaded by FPGA at power-up	Firmware upgrade	On main board	No user data is stored
Calibration backup memory Serial NOR flash 32 Mbytes	No - written only after calibration	Yes	Backup if cal factors in system memory are lost	Calibration	On main board	No user data is stored

Memory Clearing and/or Sanitization Procedures

Table 3 Acquisition / Display memory

Description and purpose	Used to store acquired waveforms when the oscilloscope is powered on
Memory clearing	Memory is cleared upon power down
Memory sanitization	Not necessary
Memory removal	Not necessary

Table 4 P700 CPU ram

Description and purpose	Operating system variables and GUI information when powered on
Memory clearing	Memory is cleared upon power down
Memory sanitization	Not necessary
Memory removal	Not necessary

Table 5 P700 system memory

Description and purpose	Main persistent memory used to store system firmware, applications, calibration data and user data
Memory clearing	User data via **Secure Erase** or **Factory Reset**
Memory sanitization	User data via **Secure Erase** or **Factory Reset**
Memory removal	No

Table 6 NOR Flash parts (2)

Description and purpose	FPGA firmware and backup for calibration factors
Memory clearing	Not necessary
Memory sanitization	Not necessary
Memory removal	Not necessary

To perform a Secure Erase

1. From the oscilloscope's main menu, select **Control > Default...**.
2. In the Default dialog box, you have these options:
   - Option A: select **Factory Reset** – A confirmation message appears. The "factory reset" deletes user data from the eMMC without performing the NISPOM sanitation procedure. It deletes files by removing entries in the file system directory structure (like any ordinary file removal in any operating system). So with special tools, following a "factory reset", user data might be recoverable. The "factory reset" procedure takes a few minutes.
   - Option B: select **Secure Erase** – A confirmation message appears. The "secure erase" performs a NISPOM sanitation procedure that erases user data and prevents it from being recovered. The "secure erase" procedure may take hours.
3. The oscilloscope will reboot when finished.

NOTE

With both the **Factory Reset** and **Secure Erase** procedures:

- The Licenses are maintained. There is no user-specific information in license files.
- The calibration results are stored in an external NOR eprom on the main board. This is not erased. There is no user-specific information in the calibration data.
- The FPGA programming memory is stored in an external NOR eprom on the main board. This is not erased. There is no user-specific information in the FPGA eprom.
- The instrument is returned to the state it was in when received by the customer. However, if the version of InfiniiVision firmware (including FPGA programming) was updated since it was received, this will not be reset. There is no user data related to these updates.

User and Remote Interface Security Measures

Under the menu **Utilities > User Options...** is an **Enhanced Security** tab.

The user can purchase a license that allows the disabling of access to the USB ports, the LAN interface, and other Remote access as well as disabling storage of user data. See the *User's Guide* for more information.

If this license is not installed, understand the following about USB mass storage device security and remote access interfaces.

USB Mass Storage Device Security

The user is responsible for providing security for the I/O ports for remote access by controlling physical access to the USB ports.

Remote Access Interfaces

The user is responsible for providing security for the I/O ports for remote access by controlling physical access to the I/O ports. The instrument should be connected only to a secure network or left unconnected. The I/O ports must be controlled because they provide access to all user settings, user states, and the display images.

The I/O ports include USB device and LAN.

Procedure for Declassifying a Faulty Instrument

If the oscilloscope is not functioning and it needs to be declassified, contact Keysight technical support.