DAQ970A/DAQ973A
Data Acquisition System

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

KEYSIGHT

SECURITY GUIDE

Table of Contents

Notices

Copyright notice

Manual Part Number

DAQ97-90003

Edition

Edition 3, October 2024

Published by

Keysight Technologies
Bayan Lepas Free Industrial Zone
11900 Bayan Lepas, Penang
Malaysia

Software Revision

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates and the latest documentation for your product, go to the product page at:

- www.keysight.com/find/DAQ970A
- www.keysight.com/find/DAQ973A

A portion of the software in this product is licensed under terms of the General Public License Version 2 (GPLv2). The text of the license and source code can be found at www.keysight.com/find/GPLV2.

This product uses Microsoft Windows CE. Keysight highly recommends that all Windows-based computers connected to Windows CE instruments use current anti-virus software. For more information, go to the respective product page at:

- www.keysight.com/find/DAQ970A
- www.keysight.com/find/DAQ973A

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 Licenses

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.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Keysight Technologies' standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c) (1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Waste Electrical and Electronic Equipment (WEEE)

This product complies with the European WEEE directive marketing requirement. The affixed product label (see below) indicates that you must not discard this electrical/electronic product in domestic household waste.

Product Category: With reference to the equipment types in the European WEEE directive Annex 1, this product is classified as "Monitoring and Control instrumentation" product. Do not dispose in domestic household waste.

To return unwanted products, contact your local Keysight office, or see http://about.keysight.com/en/companyinfo/environment/takeback.shtml for more information.

Declarations of Conformity

Declarations of Conformity for this product and for other Keysight products may be downloaded from the Web. Go to https://regulations.about.keysight.com/DoC/default.htm, you can then search by product model number to find the latest Declaration of Conformity.

Safety Information

WARNING	The WARNING sign denotes a hazard. It calls attention to a procedure, practice, or the like, which, if not correctly performed or adhered to, could result in personal injury. Do not proceed beyond a WARNING sign until the indicated conditions are fully understood and met.
CAUTION	The CAUTION sign denotes a hazard. It calls attention to an operating procedure, or the like, which, if not correctly performed or adhered to, could result in damage to or destruction of part or all of the product. Do not proceed beyond CAUTION sign until the indicated conditions are fully understood and met.
NOTE	The NOTE sign denotes important information. It calls attention to a procedure, practice, condition or the like, which is essential to highlight.

Warranty

This Keysight Technologies product is warranted against defects in material and workmanship for a period of one year from the date of shipment. During the warranty period, Keysight Technologies will, at its option, either repair or replace products that prove to be defective. For warranty service or repair, this product must be returned to a service facility designated by Keysight Technologies. Buyer shall prepay shipping charges to Keysight Technologies, and Keysight Technologies shall pay shipping charges to return the product to Buyer. For products returned to Keysight Technologies from another country, Buyer shall pay all shipping charges, duties, and taxes.

Where to find the latest information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, see the following URL:

- http://www.keysight.com/find/DAQ970A
- http://www.keysight.com/find/DAQ973A

To receive the latest updates by email, subscribe to Keysight Email Updates:

- http://www.keysight.com/find/MyKeysight

Information on preventing instrument damage can be found at:

- http://www.keysight.com/find/PreventingInstrumentRepair

Is your product software up-to-date?

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates for your product, go to the Keysight Technical Support website at:

- http://www.keysight.com/find/techsupport

Contacting Keysight Sales and Service Office

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

Product family name	Product name	Model number
Data Acquisition Unit	Data Acquisition System	DAQ970A/DAQ973A
Data Acquisition Unit	20-Channel FET Multiplexer Module	DAQM900A
Data Acquisition Unit	20-Channel Armature Multiplexer Module	DAQM901A
Data Acquisition Unit	16-Channel Reed Multiplexer Module	DAQM902A
Data Acquisition Unit	20-Channel Actuator/General-Purpose Switch Module	DAQM903A
Data Acquisition Unit	4×8 Two-Wire Matrix Switch Module	DAQM904A
Data Acquisition Unit	Dual 1:4 RF Multiplexer (50 Ω) Module	DAQM905A
Data Acquisition Unit	Multifunction Module	DAQM907A
Data Acquisition Unit	40-Channel Single-Ended Multiplexer Module	DAQM908A
Data Acquisition Unit	4-Channel 24-Bit Digitizer Module	DAQM909A
Data Acquisition Unit	20-Channel Low-Voltage Armature Multiplexer Module	DAQM910A

Document Purpose

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

For more 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.

Security Terms and Definition

Term	Definition
Clearing	As defined in Section 8-301a of DoD 5220.22-M, 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 procedure that must be undertaken before an instrument can be removed from a secure environment, such as when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. Keysight Technologies's declassification procedures are designed to meet the requirements specified in DoD 5220.22-M, Chapter 8.
Sanitization	As defined in Section 8-301b of DoD 5220.22-M, 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. Keysight Technologies's memory sanitization procedures 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 5.2.5.5.5 of the ISFO Process Manual.
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight Technologies's 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 1-1: Summary of 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
Processor DDR3 SDRAM 256 MByte	Yes	No	Contains working copies of operating system, instrument software and measurement data. It also offers a RAM backed file system.	Operating system	Mainframe	Power cycle
Parallel NAND Flash Memory 256 MByte	Yes	Yes	Contains Microsoft Windows CE Embedded Operating System, instument firmware, crash recovery image, connectivity data, FPGA configuration image and user instrument states. It also serves as the boot flash	Programmed before installed, by firmware operations, and by user input	Mainframe	Refer to Table 1-2
I2C EEPROM 4 kByte	No	Yes	Contains board revision, MAC address and serial number.	By factory install	Mainframe	Not available
Battery-backed SRAM 128 kByte	Yes	Yes	Used to save instrument readings and instrument state.	By user input	Mainframe	Refer to Table 1-3
Processor FPGA (SRAM) 2200 kbit	Yes	No	Used for data processing.	By FPGA operations	Mainframe	Power cycle
Module Processor (FRAM) 15.5 kByte	Yes	Yes	Used to store processor execution code, calibration constants, relay counts, user label, relay states and state information.	By factory install, by firmware upgrade, by firmware operations, and by user input	Module	Refer to Table 1-4
Power Processor (FRAM) 8.5 kByte	No	Yes	Used to store processor execution code.	By factory install and by firmware upgrade	Mainframe	Not available
Keyboard Processor (FRAM) 8.5 kByte	No	Yes	Used to store processor execution code.	By factory install and by firmware upgrade	Mainframe	Not available
Measurement Processor (Flash) 512 kByte	No	Yes	Used to store processor execution code.	By factory install and by firmware upgrade	Measurement board	Not available

Measurement Processor (SRAM) 98 kByte	Yes	No	Used for data path processing	By firmware operations	Measurement board	Power cycle
Measurement Calibration (EEPROM) 8 kByte	Yes	Yes	Contains calibration data	By user input	Measurement board	Not available
Measurement FPGA (Flash) 1.27 Mbit	No	Yes	Contains logic array configuration	By factory install and by firmware upgrade	Measurement board	Not available
Measurement FPGA (SRAM) 166 kbit	Yes	No	Used for data processing	By FPGA operations	Measurement board	Power cycle
NOR Flash Memory 1 MByte	Yes	Yes	Used to store processor execution code, FPGA configuration image, calibration constants, relay counts, user label, relay states and state information.	By factory install, by firmware upgrade, by firmware operations, and by user input	Module	Refer to Table 1-5

Summary of Memory Declassification Procedures

This section explains how to clear, sanitize, and remove memory from your instrument, for all classes of memory that are writable during normal operation.

NOTE

Before beginning clearing or sanitization, be sure to write down and save the information of the instrument's option. The Secure Erase All erases the instrument's option information and this information is essential for successful restoration of the instrument's operating system.

Read this entire document before using any sanitization procedure. Failure to do so may necessitate returning the instrument to an Authorized Keysight Service Center for firmware downloads and recalibration.

Table 1-2: Parallel NAND Flash Memory

Description and purpose	This memory is used to store Microsoft Windows CE Embedded Operating System, instrument firmware, crash recovery image, connectivity data, FPGA configuration image, and user instrument states. This also serve as the boot flash so here is no separate BIOS memory chip on the board.
Size	256 MByte

Memory cleaning	Front panel:
	To remove individual file from the internal file system, press:
	[Save Recall] > Manage Files > Action > Delete > Browse.
	Then select the file and press Select > Perform Delete.
	
	To remove all files from the internal file system, press:
	[Save Recall] > Manage Files > Action > Delete > Browse.
	Then select Internal and press Select > Perform Delete.
	
	Remote interface:
	To remove files and folders from the file system, send below commands:
	`MMEMory:DELete <file>`
	`MMEMory:RDIRectory <folder>`
	For more information, see *DAQ970A/DAQ973A Programming Guide*.

Memory sanitization	This memory can be sanitized by following the instructions in Secure Erase All. The model number, FPGA configuration image and the instrument firmware are retained. The connectivity data and user instrument state are sanitized. After reboot, the connectivity data will be restored to the factory defaults. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory removal	Not available
Memory validation	Not available

Table 1-3: Battery-backed SRAM

Description and purpose	Memory used to store instrument readings and instrument state. It is not cleared when power is turned off.
Size	128 kByte
Memory cleaning	This memory can be cleared by following the instructions in Secure Erase All. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory sanitization	This memory can be sanitized by following the instructions in Secure Erase All. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory removal	Not available
Memory validation	Not available

Table 1-4: Module Processor (FRAM)

Description and purpose	This memory is used to store processor execution code, calibration constants, relay counts (used for instrument service and maintenance), user label, relay states. DAQM907A has additional DIO output values, masks, patterns, modes, totalizer count, DAC calibration constants, modes and values.
Size	15.5 kByte
Memory cleaning	This memory can be cleared by following the instructions in Secure Erase All. The processor execution code, calibration constants and relay counts are retained. The user label, relay states, DIO output values, masks, patterns., modes, totalizer count, DAC modes and values are cleared. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory sanitization	This memory can be sanitized by following the instructions in Secure Erase All. The processor execution code, calibration constants and relay counts are retained. The user label, relay states, DIO output values, masks, patterns., modes, totalizer count, DAC modes and values are sanitized. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory removal	Not available
Memory validation	Not available

Table 1-5: NOR Flash Memory

Description and purpose	This memory is used to store processor execution code, FPGA configuration image, calibration constants, relay counts (used for instrument service and maintenance), user label and relay states.
Size	1 MByte
Memory cleaning	This memory can be cleared by following the instructions in Secure Erase All. The processor execution code, FPGA configuration image, calibration constants and relay counts are retained. The user label and relay states are cleared. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory sanitization	This memory can be sanitized by following the instructions in Secure Erase All. The processor execution code, FPGA configuration image, calibration constants and relay counts are retained. The user label and relay states are sanitized. This procedure complies with requirements in Chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specially, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.
Memory removal	Not available
Memory validation	Not available

Memory Sanitization Procedure

Secure Erase All

Erases all user-accessible instrument memory and restarts the instrument. The instrument's security settings must be unlocked to perform this action. Executing this operation will increment the instrument's secure count. This procedure should be performed only when the instrument is to be removed from a secure area.

Front panel	Remote interface
Press [Utility] > Security > Secure On > NISPOM Sanitize > Sanitize	`SYSTEM:SECurity:IMMediate`

User and Remote Interface Security Measures

Administrative Password

To defeat or override an instrument's administrative password (calibration secure override/Security option override) follow the procedure in the DAQ970A/DAQ973A Service Guide. This involves removing power and other connections to the instrument, removing the instrument cover (requires tools), shorting a jumper and cycling power. The calibration count and secure count will increase when the password is defeated using this method.

When setting a new password, the new password must start with a letter and may contain up to 12 letters (A-Z), digits (0-9), or underscore character (_). The password never expires.

This instrument does not track or report invalid password attempts, nor does it lock-out password entry following a number of invalid password entries.

Remote Access Interface

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 I/O ports must be controlled because they provide access to all user settings, user states, and the display image. The I/O ports include USB, LAN and GPIB interfaces.

Modifying these settings requires the instrument password. The secure count will increase when a remote interface is disabled or enabled.

The LAN port provides the following services, which can be selectively enabled (On) or disabled (Off): LAN, VXI-11, Sockets, Telnet, Web, mDNS, and HiSLIP.

To enable/disable LAN services:

Front panel	Remote interface
Press [Home] > User Settings > I/O > LAN Settings > LAN Services	`SYSTEM:COMMunicate:ENABle {ON|OFF}, <interface>` where `<interface> = {USB|LAN|SOCKets|TELNet|VXI11|WEB|USBMtp|USBHost|HISLip}` For mDNS, send this command: `LXI:MDNS:ENABle {ON|OFF}`

To enable/disable USB interface:

Front panel	Remote interface
Press [Home] > User Settings > I/O > USB Settings > USB SCPI Off/On	`SYSTEM:COMMunicate:ENABle {ON|OFF}, USB`

To enable/disable GPIB interface (for DAQ973A only):

Front panel	Remote interface
Press [Home] > User Settings > I/O > GPIB Off/On	`SYSTem:COMMunicate:ENABle {ON|OFF},GPIB`

USB device MTP (Driverless) connection device

Front panel	Remote interface
Press [Home] > User Settings > I/O > USB Settings > File Access Off/On	`SYSTEM:COMMunicate:ENABle {ON|OFF}, USBMTP`

Note: This requires that the instrument is unlocked. The secure count will increase when this port is disabled or enabled.

Front panel USB host port

Front panel	Remote interface
Press [Save Recall] > Log to USB > Logging Off/On	`SYSTEM:USB:HOST:ENABle {ON|OFF}`

Note: This requires that the instrument is unlocked. The secure count will increase when this port is disabled or enabled.

Front panel display

To provide basic security, you may disable the front panel display.

To disable the display on the front panel, press [Home] > User Settings > Display Options > Display Off.

NOTE When disabled, press any key to turn the display back on.

How to disable the front panel during remote operation

To programmatically lock out all front panel operation and remote access over the current interface, use the `SYSTem:LOCK` command. For more information, see *DAQ970A/DAQ973A Programming Guide*.

Calibration regulation

The instrument requires a password to unsecure the instrument before performing calibration. The instrument's calibration count will increment with each successful calibration step.

On the front panel, press [Utility] > Calibrate > Perform Cal Step.

Firmware update regulation

The instrument requires a password to unsecure the instrument before updating firmware. The instrument's calibration count will increment with each successful update.

To view the current installed firmware version, press [Home] > Help > About.

To update a new firmware version, press [Utility] > Admin > Firmware Update.

Procedure for Declassifying a Faulty Instrument

If the instrument is not functioning and the user is unable to use the front panel or the remote interface to declassify the instrument, the user must physically remove the front panel printed circuit assembly from the instrument. Once this assembly is removed, proceed with one of these options:

- Destroy the front panel printed circuit assembly using a DSS/NISPOM approved destruction method, OR
- Remove the NAND flash memory component (U302) and SRAM memory component (U403) located on the front panel printed circuit assembly, and destroy them using a DSS/NISPOM approved destruction method.

For module, the user must physically remove the module's printed circuit assembly from the instrument. Once this assembly is removed, proceed with one of these options:

- Destroy the module's printed circuit assembly using a DSS/NISPOM approved destruction method, OR
- Remove the MSP430 processor component located on the module card printed circuit assembly, and destroy it using a DSS/NISPOM approved destruction method.
- For DAQM909A, remove the NOR flash memory component (U303) located on the module card printed circuit assembly, and destroy it using a DSS/NISPOM approved destruction method.

Refer to the procedures in *DAQ970A/DAQ973A Service Guide* for removing the front panel circuit assembly.

Send the instrument to a Keysight repair facility. If the unit is still under warranty, the repair facility will replace the front panel printed circuit assembly. If this restores instrument functionality, the user will not be charged for the new assembly. If a different assembly is at fault, the user will be charged for the new front panel assembly even though the instrument is still under warranty.

References

1. DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)” United States Department of Defense. Revised February 28, 2006.

   May be downloaded in Acrobat (PDF) format from:
   https://www.dss.mil/ma/ctp/io/fcb/nisp/

2. ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Defense Security Service.

   DSS-cleared industries may request a copy of this document via email, by following the instructions at:
   https://www.dss.mil/contact/knowledge_center/

Edition 3, October 2024
Printed in Malaysia
DAQ97-90003
www.keysight.com