TMS470R1VF48C JTAG Security Module (JSM) Reference Guide

Literature Number: SPNU245
February 2005

TEXAS INSTRUMENTS

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and application s using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different form or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Interface	interface.ti.com	Digital Control	www.ti.com/digitalcontrol
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
		Telephony	www.ti.com/telephony
		Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265

REVISION HISTORY

REVISION	DATE	NOTES
*	2/05	Initial version of document.

Contents

Table

JTAG Security Module (JSM)

The JTAG security module (JSM) secures internal memory by disabling the JTAG and memory test ports of TMS470R1VF devices when enabled.

Topic **Page**

1 Features

The JSM module design includes the following features:

- ❏ The 64-bit JSM enable key is located in flash memory.
- ❏ Access to the ARM CPU via JTAG scan is disabled when the JSM enable key is modified.
- ❏ Access to internal memory by the TI parallel memory test bus is disabled when the JSM enable key is modified.
- ❏ Access to the TI peripheral scan chain is limited to only the JSM scan path unless a special factory test scan password is entered.

Table 1 summarizes the options available for the JSM when used with the memory security module (MSM).See *TMS470R1x Memory Security Module Reference Guide* (literature number SPNU246) for more information about the MSM.

Table 1. Summary of Options for JSM

Condition of MSM	JSM Disabled	JSM Enabled
Disabled	- No code security is available. - Peripheral scan chain is blocked	- Full security (except for expansion bus) is on. - Debug capability is disabled. - Security cannot be disabled. - Peripheral scan chain is blocked.
Enabled	- Full security is on. - Debugging is allowed for out-of-zone memory and peripherals. - Security can be disabled by matching user programmed password. - Peripheral scan chain is blocked.	-Full security (including expansion bus) is on. - Debug capability is disabled. - Security cannot be disabled. - Peripheral scan chain is blocked.

2 Operation

The JSM defines a location in flash memory that contains an enable key. This 64-bit location can be in the customer one-time programmable (OTP) flash memory or in the first bank of the main flash array. Please see the specific device data sheet for the location of the enable key.

The enable key location is programmed by TI at device initial test time with a specific enable value known as the *visible unlock code*. At device reset, this value is automatically read. If the value is correct, access is allowed to the CPU JTAG scan chain or the parallel memory test (PMT) bus. If any bit has been altered, JTAG and PMT access is blocked.

The JSM may be used alone or with the memory security module (MSM) to provide different levels of device security. See *TMS470R1x Memory Security Module Reference Guide* (literature number SPNU246) for more information about the MSM.

2.1 Engaging Security

Engage security by programming the enable key. Typically, the enable key is programmed to all zeros. You should do this after programming and verifying the code in the device. You can verify the enable key location after programming because the device does not lock until reset is asserted.

2.2 Disabling Security

Once security has been enabled, you can only disable it by restoring the visible unlock code to the enable key location. If the enable key location is in OTP flash memory, the security cannot be disabled. If the enable key location is in the main flash array, the sector containing the key location must be erased and the visible unlock code must be programmed into this location. If the routines to do this are not already part of the user code, security cannot be disabled because the routines cannot be loaded externally.

3 Use With Memory Security Module (MSM)

The JSM may be used alone or with the MSM.

3.1 When the JSM Is Required

Whenever code security is needed, the JSM is required. Whenever the MSM is used on a device, the JSM is also included. The JSM disables the peripheral scan chain even if JSM security has not been engaged, thus prohibiting disabling the MSM from scanning the peripheral scan path.

3.2 When the MSM Is Required

If any of the three following conditions apply, then the MSM must be included on the device with the JSM:

- ❏ The device has an expansion bus.

  If the device has an expansion bus and code is executed from the expansion bus, the MSM is required with the JSM. The MSM prevents a hacker from replacing the external memory device with one that has a routine for dumping the contents of internal memory.

- ❏ The ability to debug the device after security is enabled is required.

  If the ability to do JTAG emulation on a device after security has been enabled is required, then the MSM should be used and the JSM should not be enabled. Once the JSM is enabled, emulation is blocked.

- ❏ The ability to disable security after it has been enabled is required.

  If the ability to do JTAG emulation on a device after security has been enabled is required, then the MSM should be used and the JSM should not be enabled. After the JSM is enabled, it cannot be disabled unless the sector containing the enable key can be erased and the visible unlock code can be programmed back into this location.