Application Report
SPNA146–February 2012

Verification of Data Integrity Using CRC

Hari Udayakumar

ABSTRACT

The purpose of this application report is to provide help setting up the cyclic redundancy check (CRC) controller of the Hercules™ TMS570 and RM4 microcontrollers. The Hercules microcontrollers from Texas Instruments are 32-bit RISC microcontrollers based on the ARM® Cortex™-R4 core with an advanced architecture and a rich peripheral set that supports on-chip diagnostics to aid developers of safety-oriented systems.

Contents

List of Figures

1 Introduction

1.1 MCRC Controller

The MCRC controller is a module that is used to perform CRC to verify the integrity of memory system. A signature, representing the contents of the memory, is obtained when the contents of the memory are read into the MCRC controller. The responsibility of the MCRC controller is to calculate the signature for a set of data and then compare this value against a pre-determined good signature value.

1.2 Main Features

The Hercules CRC controller offers:

- Four channels to perform background signature verification on any memory sub-system, RAM or Flash
- Data compression on 8-, 16-, 32-, and 64-bit data size
- Maximum-length Parallel Signature Analysis Register (PSA) constructed based on a 64 bit primitive polynomial
- Each channel has a CRC Value Register (CRC_REG) that contains the predetermined CRC value
- Event trigger from timer to initiate DMA data transfer
- Programmable 20-bit pattern counter-per-channel to count the number of data patterns for compression
- Three modes of operation: auto, semi CPU and full CPU
- For each channel, CRC can be performed either by MCRC controller or by CPU
- Automatically perform signature verification without CPU intervention in AUTO mode
- Generate interrupt to CPU in semi-CPU mode to allow CPU to perform signature verification itself

- Generate CRC fail interrupt in AUTO mode if signature verification fails
- Generate Timeout interrupt if CRC is not performed within the time limit
- Generate DMA request per channel to initiate CRC value transfer

1.3 MCRC Block Diagram

Figure 1 gives a detailed view of the MCRC internal architecture. The MCRC controller provides four channels to perform CRC calculation on multiple memories in parallel and can be used on any memory system. Channel 1 can also be put into data-trace mode. In data-trace mode, the MCRC controller compresses each data being read through the CPU read data bus.

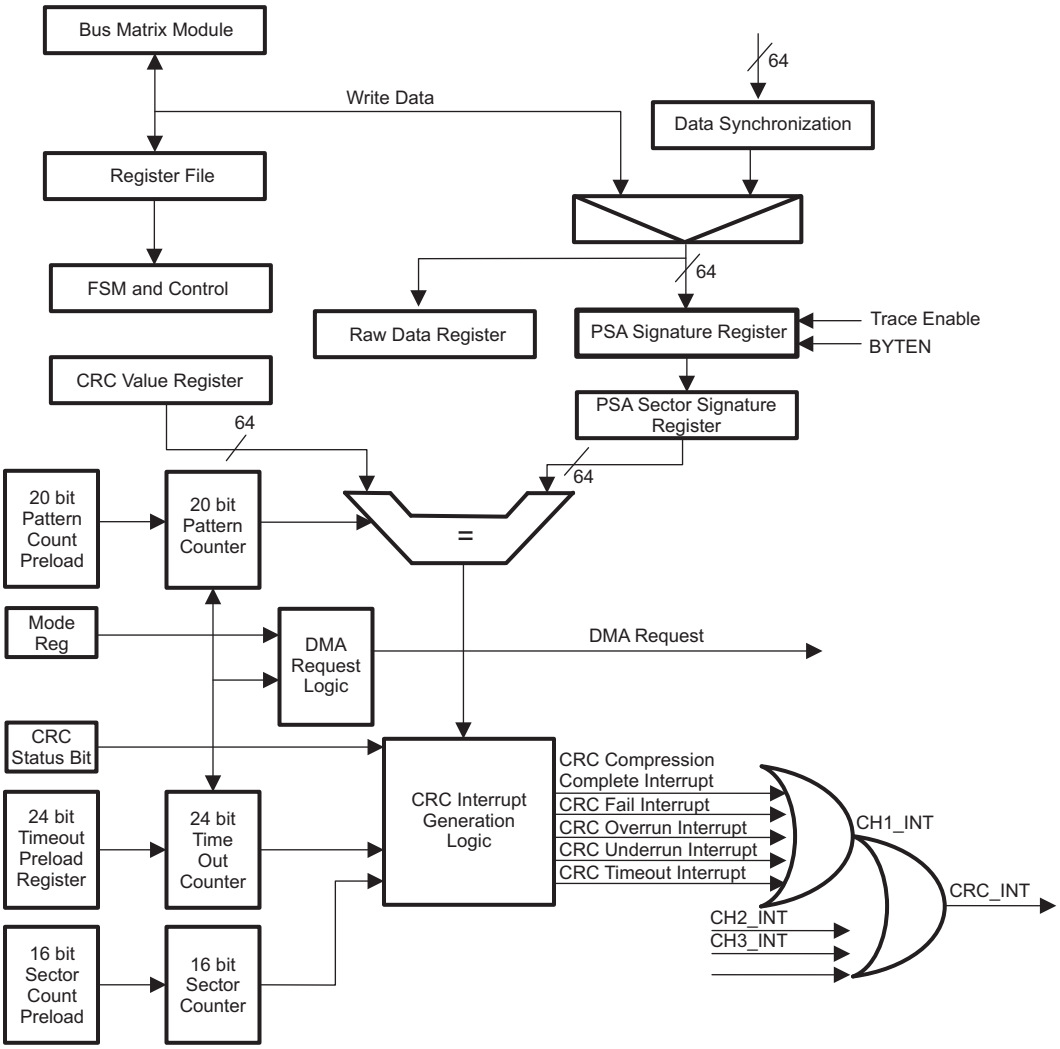

Figure 1. MCRC Internal Architecture

2 Verification of Data Integrity Using MCRC

This section describes the configuration of the MCRC controller for verification of data integrity before the data transfers between different memory locations.

The Hercules microcontroller is configured with the following parameters for the data transfer between two RAM locations:

- MCRC controller in auto mode
- DMA configured for software trigger

- Successful signature verification triggers a software DMA request for data transfer between Memory1 and Memory2

2.1 Circuit Diagram

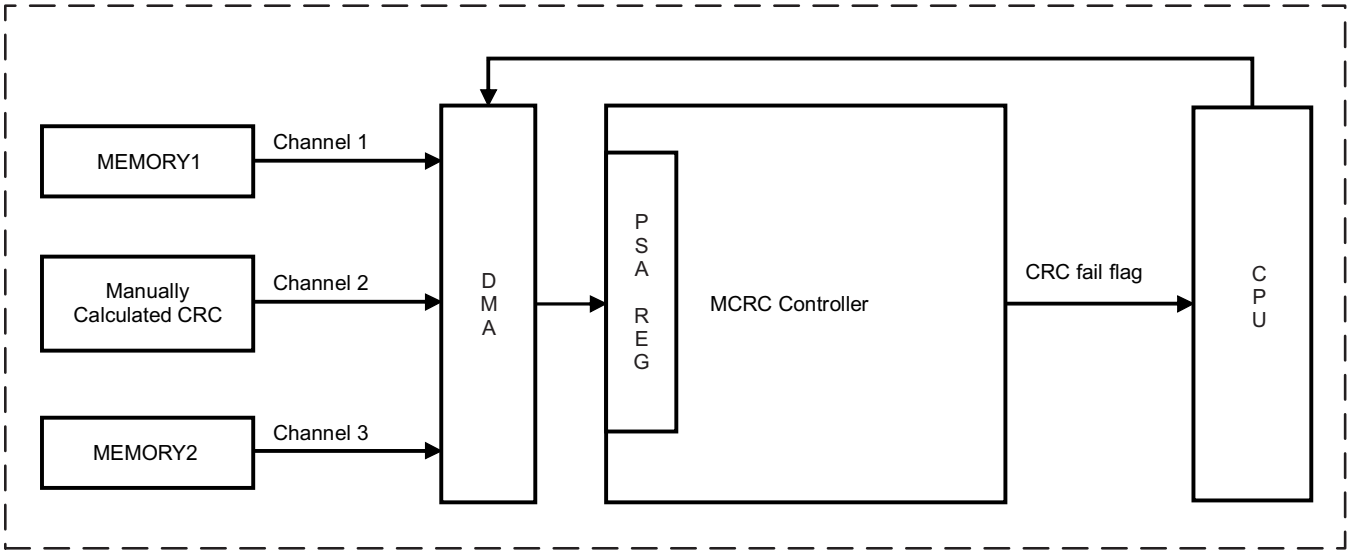

Figure 2. Verification of Data Integrity Using MCRC Controller

2.2 MCRC Controller Setup

The MCRC controller provides four channels to perform CRC calculation on multiple memories in parallel and can be used on any memory system. Channel 1 can also be put into data-trace mode. In data-trace mode, MCRC controller compresses each data being read through the CPU read data bus.

The following configuration needs to be done for the MCRC controller for verifying data integrity.

- MCRC controller reset
- Configure the Pattern Count Register (PCOUNT_REG) and the Sector Count Register (SCOUNT_REG)
- Configure the mode of operation of the MCRC controller
- Configure the interrupts

2.2.1 MCRC Controller Reset

The MCRC controller should be reset before configuring the MCRC controller for the verification of data integrity. The reset condition resets the PSA Signature Register (PSA_SIGREG). Writing a 1 to the channel (x) PSA software reset bit in the Global Control Register (GCTRL) resets the corresponding PSA signature register for that CRC channel (x).

The following code snippet shows the CRC reset condition for channel 1.

```
*GCTRL = 0x01;
```

2.2.2 Configuring MCRC Controller Registers and Counters

- PSA Signature Register: This register can be both read and written. When it is written, it can either compress the data or just capture the data depending on the state of CHx_MODE bits. When the PSA signature register is read, it gives the calculated signature. Each time PSA signature register is written, a signature is generated. The MCRC controller supports doubleword, word, half word and byte access to the PSA signature register. During a non-doubleword write access, all unwritten byte lanes are padded with zero's before compression.

  Note that comparison between the PSA signature register and the CRC value register is always in 64 bit because a compressed value is always expressed in 64 bit.

  The PSA signature register is reset to zero under the following conditions:

  – System reset
  – PSA software reset
  – One sector of data patterns are compressed
- CRC Value Register: This register stores the pre-determined CRC value. After one sector of data patterns is compressed by the PSA signature register, the MCRC controller can automatically compare the resulting signature stored at the PSA signature register with the pre-determined value stored at the CRC value register.
- Pattern Count Registers (PCOUNT_REG): The data pattern counter is a 20 bit down counter and can be pre-loaded with a programmable value stored in the pattern count register. When the data pattern counter reaches zero automatic signature verification is performed in AUTO mode.

2.2.3 Configuring MCRC Controller Mode of Operation

The MCRC controller can operate in one of the following modes:

- AUTO Mode: In this mode, the MCRC controller, in conjunction with DMA controller, can perform CRC totally without CPU intervention. A sustained transfer of data to both the PSA signature register and the CRC value register are performed in the background of the CPU.

  When a mismatch is detected, an interrupt is generated to the CPU. A 16 bit current sector ID register is provided to identify which sector causes a CRC failure.
- Full-CPU Mode: In this mode, the CPU does the data patterns transfer and signature verification all by itself. CPU performs data patterns transfer by reading data from the memory system to the PSA signature register. After a certain number of data patterns are compressed, the CPU can read from the PSA signature register and compare the calculated signature to the pre-determined CRC signature value.

  In full-CPU mode, neither interrupt nor DMA request is generated. All counters are also disabled.

2.2.4 Configuring MCRC Controller Interrupts

MCRC generates several types of interrupts per channel. There is an interrupt enable bit associated with each interrupt. However, no interrupt is generated in full-CPU mode.

- CRC fail interrupt is generated in AUTO mode only. When the signature verification fails, the CRC fail flag is set; the CPU should take action to address the fail condition and clear the CRC fail flag after it resolves the CRC mismatch.
- Overrun Interrupt is generated if a CRC fail is detected then the current sector number is recorded in the current sector register. If the CRC fail status bit is not cleared and the current sector register is not read by the host CPU before another CRC fail is detected for another sector, then an overrun interrupt is generated.
- An under-run interrupt only occurs in AUTO mode. The interrupt is generated when the CRC value register is not updated with the corresponding signature when the data pattern counter finishes counting.

- Timeout interrupt ensures that the memory system is examined within a pre-defined time frame and no loss of incoming data. There is a 24-bit timeout counter per CRC channel. The 24-bit timeout down counter can be pre-loaded with two different pre-load values: watchdog timeout pre-load value (CRC_WDTOPLDx) and block complete timeout pre-load value (CRC_BCTOPLDx).
  - Watchdog Timeout Pre-load Register (CRC_WDTOPLDx) is used to check if DMA does supply a block of data responding to a request in a given time frame.
  - Block Complete Timeout Pre-Load Register (CRC_BCTOPLDx) is used to check if one complete block of data patterns are compressed within a specific time frame.

2.3 DMA Controller Setup

The MCRC controller is used in AUTO mode here on the DMA request for data transfer from the Memory 1 for signature calculation and another DMA request for signature verification. On successful signature verification, a third DMA request is generated for the actual data transfer from memory 1 to memory 2.

The DMA controller configuration: For channel 1 signature calculation.

- Source address: Memory 1 to be verified
- Destination address: Channel 1 PSA signature register
- Source addressing mode: Post increment addressing mode
- Destination addressing mode: Constant addressing mode
- Trigger type: Software trigger from CPU
- Autoinitiation disabled

The DMA controller configuration: For channel 2 for signature verification.

- Source address: Memory 1
- Destination address: CRC value register
- Source addressing mode: Constant addressing mode
- Destination addressing mode: Constant addressing mode
- Trigger type: Hardware trigger from CPU
- Autoinitiation disabled

The DMA controller configuration: For channel 3 for data transfer from memory 1 to memory 2.

- Source address: Memory 1
- Destination address: Memory 2
- Source addressing mode: Post increment addressing mode
- Destination addressing mode: Post increment addressing mode
- Trigger type: Software trigger from CPU
- Autoinitiation disabled

2.4 MCRC Controller Working

The PSA signature register compresses an incoming data pattern into a signature when it is written. When one sector of data patterns are written into PSA signature register, a final signature corresponding to the sector is obtained. The CRC value register stores the pre-determined signature corresponding to one sector of data patterns. The calculated signature and the pre-determined signature are then compared to each other for signature verification. To minimize the CPU's involvement, data patterns transfer can be carried out at the background of the CPU using the DMA controller. The 64-bit PSA signature register is based on the primitive polynomial found in Equation 1 to produce the maximum Length Linear Feedback Shift Register (LFSR).

$$f(x) = x64 + x4 + x3 + x + 1 \quad (1)$$

The incoming data pattern to the PSA signature register is typically initiated by the DMA master. When DMA is properly setup, it would read data from the pre-determined memory system and write them to the memory mapped PSA signature register. Each time the PSA signature register is written, a signature is generated. The CPU itself can also perform data transfer by reading from the memory system and perform write operation to the PSA signature register if the CPU has enough throughputs to handle data patterns transfer. After system reset and when AUTO mode is enabled, the MCRC controller automatically generates a DMA request to request the pre-determined CRC value corresponding to the first sector of memory to be checked.

In AUTO mode, when one sector of data patterns is compressed, the signature stored at the PSA signature register is first copied to the PSA Sector Signature Register (PSA_SECSIGREG) and the PSA signature register is then cleared out to all zeros. An automatic signature verification is then performed by comparing the signature stored at the PSA sector signature register to the CRC value register. After the comparison, the MCRC controller can generate a DMA request. Upon receiving the DMA request, the DMA controller will update the CRC value register by transferring the next pre-determined signature value associated with the next sector of memory system. If the signature verification fails, then the MCRC controller can generate a CRC fail interrupt.

In full-CPU mode, no DMA request and interrupt are generated at all. The number of data patterns to be compressed is determined by the CPU itself. Full-CPU mode is useful when the DMA controller is not available to perform background data patterns transfer. The OS can periodically generate a software interrupt to the CPU and use the CPU to accomplish data transfer and signature verification.

2.5 Configuration Steps for Data Transfer Between Peripherals Using DMA

Configure the MCRC controller:

1. Reset the MCRC
2. Initialize the pattern count register
3. Initialize the sector count register
4. Configure the mode of the CRC channel
5. Configure the time out registers
6. Configure the MCRC interrupts

Configure the DMA controller:

1. Reset the DMA
2. Initialize the DMA RAM
3. Enable the DMA controller
4. Configure the DMA channel 1
5. Configure the DMA channel 2
6. Begin the data integrity verification by generating software DMA request for DMA channel 1.
7. Start the data transfer by generating the software DMA request for DMA channel 2 on successful signature verification.

2.6 Software Listing and Description

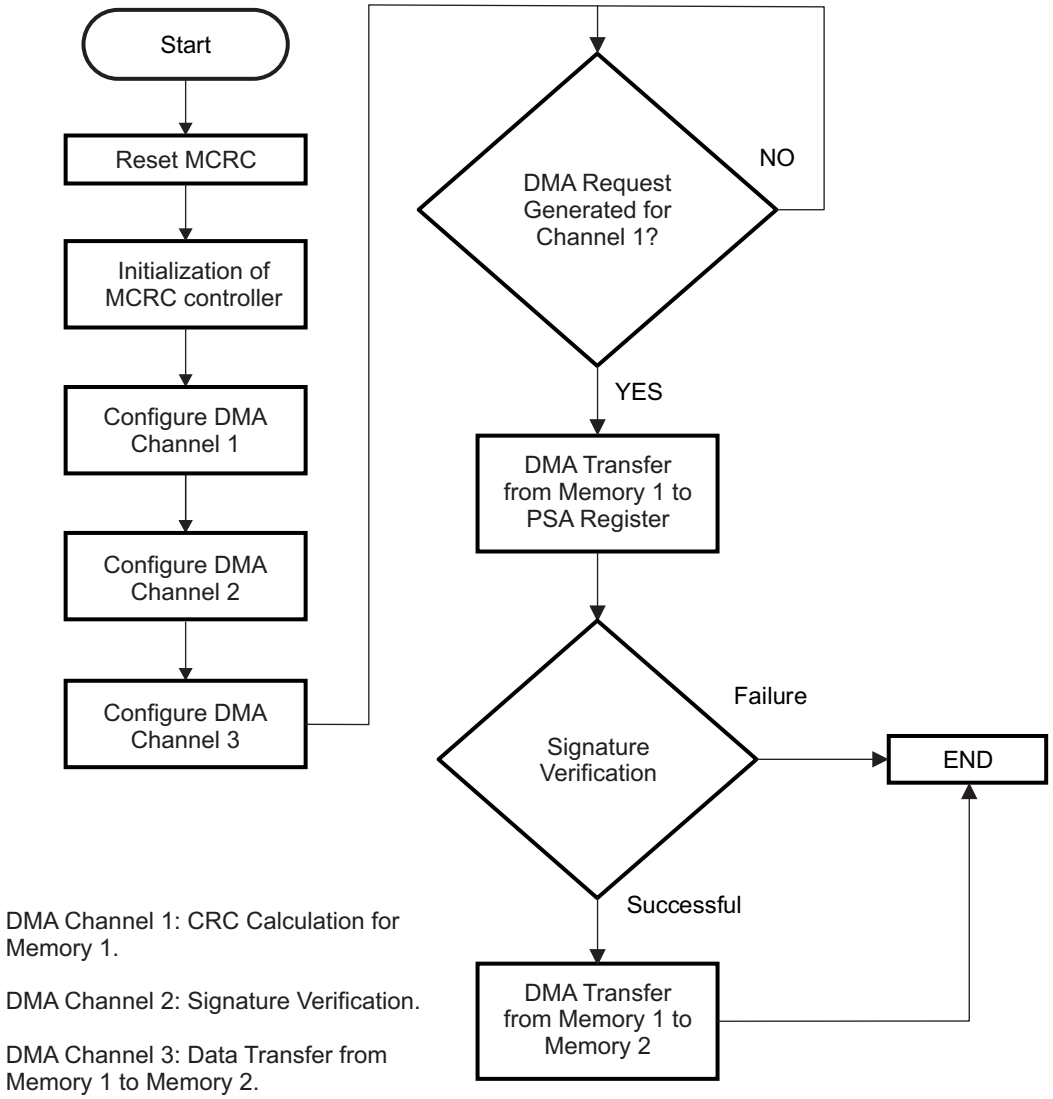

Figure 3. Software Flow

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 applications 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 TI 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. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from 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.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

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

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Mobile Processors	www.ti.com/omap		
Wireless Connectivity	www.ti.com/wirelessconnectivity		
	TI E2E Community Home Page		e2e.ti.com

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