AN2791

Booting from External Non-Volatile Memory (NVM) on SAMA5D2 MPU

Introduction

This document describes the boot process of the SAMA5D2 Arm® Cortex®-A5 based microprocessors (MPU).

MPUs, unlike MCUs, do not feature Flash memory, and thus depend on external Non-Volatile Memories (NVM) of different kinds for the boot processes.

An on-chip ROM contains an initial boot program to launch an in-system programmer that allows a PC to load the NVM with the user application and setup the boot process. Microchip's SAM Boot Assistant (SAM-BA®) tools write the user application into the external NVM and set up the boot while running on the PC and connected to the SAMA5D2 in the system through a USB, RS-232 or JTAG link.

Secure SAM-BA tools are available to enable and configure the Secure Boot mode on the SAMA5D2, which builds a root of trust for the boot chain.

Finally, this document presents the supported types of external NVMs for the boot and discusses the technical aspects of booting from external NVMs on the SAMA5D2 MPU.

Reference Documents

Document Type	Document Title	Literature Number	Available
Data Sheet	SAMA5D2 Series	DS60001476	www.microchip.com

Table of Contents

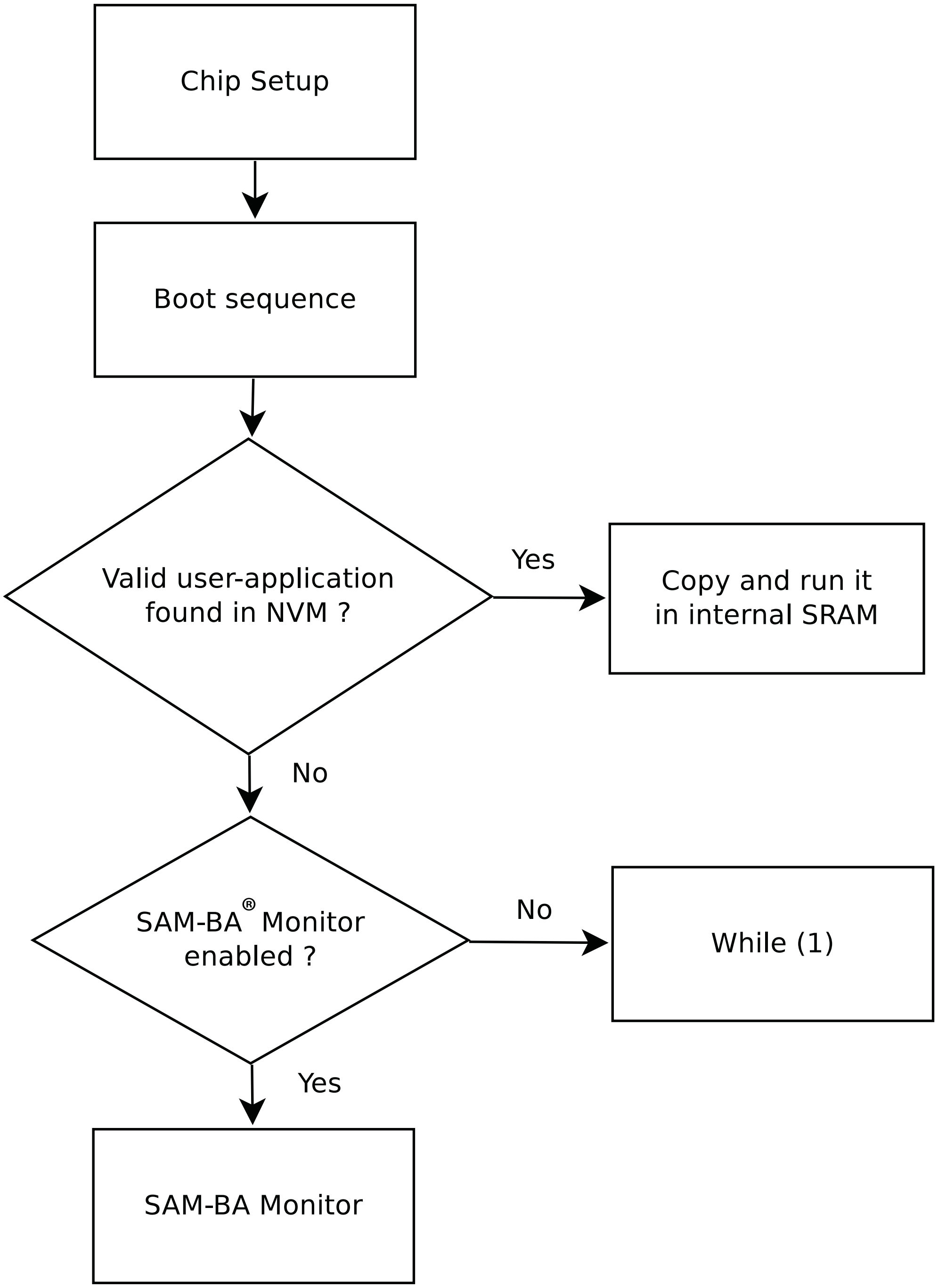
1. Role of the ROM Code

The ROM code (or Boot ROM) is a small piece of mask ROM, executed on power-on or Reset, responsible for loading the user application or a second-stage bootloader from an external NVM into the internal SRAM. The size of this user application is limited, for example to 24 KB on SAM9x5 and to 64 KB on SAMA5Dx products. Once loaded into the internal SRAM, the ROM code disables all peripheral clocks it has previously enabled, sets the PIO muxing back to its Reset state and then jumps to the address of the internal SRAM so the user application is executed.

The user application should be linked so that its entry point is at the very beginning of the internal SRAM. Nevertheless, just before jumping into the user application, the ROM code also remaps the internal SRAM at address 0x0. Hence the internal SRAM can be accessed at its regular address, for example at 0x00200000 on SAMA5D2, and is mirrored at 0x0 as well. Thus when the user application places its ARM exception vector table at the very beginning of the internal SRAM, the vectors are also seen at 0x0 by the ARM core when it needs to access them.

The 6th exception vector of ARM9 and Cortex-A5 cores is reserved and the ROM code uses this 32-bit data to store the size of the user application. Actually, the ROM code fetches this value to know exactly how many bytes it should transfer from the external NVM instead of reading the maximum size allowed to the user application, hence speeding up the boot process. The ROM code also checks the other exception vector values to decide whether the user application can be considered as valid, or whether it should be skipped. The ROM code then tries to boot from the next external NVM in the boot sequence.

Figure 1-1. ROM Code Process Flow


Chip Setup
Boot sequence
Valid user-application found in NVM ?
Yes
Copy and run it in internal SRAM
No
SAM-BA® Monitor enabled ?
No
While (1)
Yes
SAM-BA Monitor

1.1 Boot Sequence

The boot sequence is an ordered list of embedded memory controllers from which the ROM code tries to boot.

For SAMA5D2 devices, this boot sequence is:

1. SDMMC1

2. SDMMC0
3. NandFlash on SMC (Static Memory Controller)
4. SPI0
5. SPI1
6. QSPI0
7. QSPI1

Depending on the product, the boot sequence can be tuned. For SAMA5D2 devices, each step of the boot sequence can be disabled by setting a proper value for the Boot Configuration Word. Refer to the SAMA5D2 Data Sheet, section “Boot Configuration Word” for details.

If no bootable user application is found, for instance during the first boot in factory when the user application has not been written yet into the external NVM, the ROM code then executes its SAM Boot Assistant (SAM-BA) monitor, which in turn waits for a connection from the SAM-BA tool.

1.2 SAM Boot Assistant (SAM-BA) In-System Programmer

The SAM-BA tools are software programs, running on a PC under Windows® or Linux®, which connect and then send commands through JTAG, USB or RS-232 to the SAM-BA monitor. This monitor is a software component of the ROM code, designed to help the customer program the user application in a supported external NVM. The SAM-BA tool may also be used to tune the boot sequence. The regular SAM-BA tool is open source and freely distributed on the Microchip website. Another set of tools, regrouped as secure SAM-BA tools, are distributed under Non-Disclosure Agreement (NDA) only and are used when the Secure Boot mode of the ROM code is enabled.

1.3 Secure Boot Mode

The Secure Boot mode extends the boot process of the ROM code to add security features and create a root of trust in the boot chain. Actually, once the Secure Boot mode is enabled, the ROM code expects the user application in the external NVM to be ciphered and signed.

Indeed, the user application is ciphered with the AES-256-CBC algorithm for confidentiality purposes and signed with either AES-256-CMAC or RSA algorithm to guarantee its integrity and authenticity.

A shared secret between the customer and the SAM-based devices, the customer key, is written once and for all in fuses or One Time Programmable (OTP) memory with the help of the secure SAM-BA tools.

The ROM code requires this customer key to decipher the user application. In the case of AES-256-CMAC, the customer key is also used to verify the signature.

Once the user application is validated and deciphered in the internal SRAM and before executing it, the ROM code drives the relevant fuse or OTP controller to forbid any further access to the customer key until the next Reset. This way the customer key cannot be extracted later by software running in the SoC.

The customer key is also ciphered and signed with the secure SAM-BA cipher tool by the customer. Next, both the ciphered/signed user application and customer key are sent to the 3rd party manufacturer responsible for the production of the customer SAM-based board design.

Then the programming of the customer boards is done by the third party manufacturer with the help of the secure SAM-BA loader tool. Only the ROM code is able to decrypt and validate the customer key received from the secure SAM-BA loader tool. So the third party manufacturer, or any other party having access to the ciphered customer key, cannot extract the plain customer key, upon which the security model relies.

2. Supported External Non-Volatile Memories (NVM)

2.1 SDCard/e.MMC Boot

SAMA5D2 devices can boot from SDCard or e.MMC memories connected to SDMMC0 or SDMMC1. Though SDMMC0 supports up to x8 bus width and SDMMC1 up to x4 bus width, the ROM code transfers data only with a x1 bus width through SDMMC_DAT0.

The ROM code also supports e.MMC boot partitions. In order to boot from one of the two e.MMC boot partitions, the BOOT_PARTITION_ENABLE field (bits[5:3]) must be set to either 0x1 (Boot partition 1 enabled for boot) or 0x2 (Boot partition 2 enabled for boot) and the BOOT_ACK bit (bit[6]) must be set to 0x1 (Boot acknowledge sent during boot operation) in byte 129 of the Extended CSD register. Also the BOOT_BUS_WIDTH field (bit[1:0]) should be set to 0x0 (x1 bus width in boot operation mode) in byte 127 of the Extended CSD register.

The ROM code first checks if some e.MMC boot partition is enabled. If so, only the first 64 KB of the enabled boot partition are read by the ROM code. If no boot partition is enabled on an e.MMC or in case of a SDCard, the boot process continues with a standard SDCard/e.MMC detection. The ROM code looks for a “boot.bin” file in the root directory of the first partition, which must be formatted with a FAT12/16/32 file system.

2.1.1 SAMA5D2 MRL B

2.1.1.1 Known Limitations

The boot from any SDMMCx controller is very erratic on SAMA5D2 MRL B, and hence should be considered as not functional.

This limitation is due to an increase in the hardware delay used for the Card Detect pin debouncing, resulting in a timeout occurring before the SDMMC reports the pin level as stable. The ROM code may then wrongly assume that no card is inserted, which prevents it from booting from any SDMMCx controller. The rate of this failure is related to the accuracy variation of the 12 MHz RC frequency, which drives the CPU clock frequency, and thus the timeout duration, whereas the SDMMC uses another source clock to count down the debouncing delay.

For a workaround, refer to the SAMA5D2 errata, Issue "ROM Code: SDMMC0 and SDMMC1 boot".

This workaround recommends to select memory controllers other than SDMMCx as the boot media.

2.1.2 SAMA5D2 MRL C

2.1.2.1 Managing the Card Detect Pins of SDMMC0 and SDMMC1

The ROM code configures the Card Detect pin in GPIO Input mode and enables the associated internal pull-up resistor before testing the level of the Card Detect pin to decide whether to boot from an SD Card or e.MMC through the SDMMC controller. Unlike SAMA5D2 MRL B, the ROM code ignores the Card Detect pin debouncing performed by the SDMMC.

A successful boot requires the Card Detect pin to be handled carefully. If the level on the Card Detect pin is low, SDCard/e.MMC access is initiated (IOs toggling). If not, no communication with SDCard/e.MMC is performed (no IOs toggling).

To summarize:

- If the ROM code should boot from a valid SDCard/e.MMC, then the Card Detect pin level must be driven low.

- Otherwise, the Card Detect pin level must be driven high.

Note: Unlike SAMA5D2 MRL B ROM code, the SAMA5D2 MRL C ROM code tries to boot from SDMMC1, then from SDMMC0, if the level of their Card Detect pin is low, even if the EXT_MEM_BOOT bit is not set in the Boot Configuration Word.
This change, introduced in SAMA5D2 MRL C parts, allows the customer to boot from SDCard without using SAM-BA tools.

Boots from SDMMC0 and SDMMC1 can be disabled by setting, respectively, bit[10] and bit[11] in the Boot Configuration Word. If the boot from SDMMCx has been disabled by setting the relevant bit of the Boot Configuration Word, then the ROM code does not attempt to test the level of the Card Detect pin and ignores this memory controller.

However, before setting those bits or any other bits or fields of the Boot Configuration Word with SAM-BA, the ROM code must first reach its SAM-BA monitor.

⚠WARNING

As long as the boot from SDMMCx has not been disabled in the Boot Configuration Word, the following patterns of behavior apply:

- If the Card Detect pin level is driven low and a valid SDCard/e.MMC is found, the ROM code boots from this SDCard/e.MMC, and hence does not reach its SAM-BA monitor.
- If the Card Detect pin level is driven low and any peripheral other than an SDCard/e.MMC is connected to the SDMMCx pins, the ROM code may be caught in an endless loop, also preventing it from reaching its SAM-BA monitor.

This must be taken into account when designing boards based on SAMA5D2 MRL C or when migrating existing designs from SAMA5D2 MRL B to SAMA5D2 MRL C.

2.2 Parallel NAND Flash Boot

The ROM code only supports 8-bit NAND Flash memories connected to the SMC; booting on 16-bit NAND Flash is not possible.

Although some NAND Flash parameters and ECC requirements can be retrieved from ONFI parameters for ONFI-compliant memories, we highly recommend writing a specific header at the beginning of the first page of the NAND Flash. This header is built from a 32-bit word repeated 52 times. The ROM code selects the 32-bit word value with the most occurrences among the 52 values. This 32-bit word encodes precisely the memory geometry and PMECC initialization settings. Refer to the SAMA5D2 data sheet, section “NAND Flash Boot: NAND Flash Detection” to get the exact layout of this 32-bit word.

2.3 SPI NOR Flash Boot

The ROM code can boot from SPI NOR Flash memories connected to SPI0 or SPI1 if the SPI NOR Flash memories are compatible with either AT25, AT26 Serial Flash or AT45 DataFlash memories. Refer to the SAMA5D2 data sheet, section “SPI Flash Boot” for more details.

2.4 QSPI NOR Flash Boot

The ROM code can boot from QSPI NOR Flash memories connected to QSPI0 or QSPI1.

Important: QSPI NAND Flash memories are not supported.

2.4.1 SAMA5D2 MRL B

QSPI NOR Flash boot is early and thus limited on MRL B. The ROM code reads the JEDEC ID with the 9Fh SPI command. The 1st byte of the JEDEC ID is the Manufacturer ID. This Manufacturer ID is used as an index in a table, hardcoded in the ROM code, to retrieve the required parameters to read data from the QSPI NOR Flash.

Only three manufacturer IDs are supported:

- 01h (Spansion/Cypress)
- 20h (Micron)
- C2h (Macronix)

Note: Other manufacturer IDs are ignored.

The ROM code jumps to the next NVM in the boot sequence. Refer to the SAMA5D2 data sheet, section “QSPI NOR Flash Boot for MRL B” for more details.

2.4.1.1 Known Limitations

If the QSPI NOR Flash memory is not in its Power-on Reset state when the SAMA5D2 is reset, the ROM code fails to boot from this memory.

This occurs when the QSPI NOR Flash memories have entered Continuous Read mode (XIP).

This can also occur when the memories have entered a stateful 4-Byte Address mode, as opposed to the stateless 4-byte address instruction set, which is supported by most recent QSPI NOR Flash memories above 128 Mbits. The ROM code assumes that the QSPI NOR Flash memory has not entered its Continuous Read mode and so can execute any regular SPI command such as the Read JEDEC ID (9Fh) command, and that the Fast Read Quad I/O (EBh) instruction is followed by a 3-byte address.

2.4.2 SAMA5D2 MRL C

2.4.2.1 Software Reset of the QSPI NOR Flash Memory

QSPI limitations of the ROM code in MRL B are fixed by:

1. raising the 4 I/O lines to high level during 12 QSPI clock cycles
2. sending a software Reset command sequence (66h, 99h)

before sending any other SPI command.

Step 1 causes the QSPI NOR Flash memory to exit its Continuous Read (XIP) mode, regardless of its manufacturer, whereas step 2 restores the Power-on Reset state, hence exiting the stateful 4-Byte Address mode.

Since the ROM code does not know the internal state of the QSPI NOR Flash memory (has it entered its SPI 4-4-4 mode?) when it tries to reset this memory, the ROM code first sends the reset command sequence (66h, 99h) with the SPI 4-4-4 protocol, to force an exit from the SPI 4-4-4 mode if needed, then sends the same reset command sequence but with the SPI 1-1-1 protocol. If the QSPI NOR Flash memory has not entered its SPI 4-4-4 mode, it should ignore the first Reset command sequence as it cannot decode it correctly.

Figure 2-1. Reset Command Sequence in SPI 4-4-4

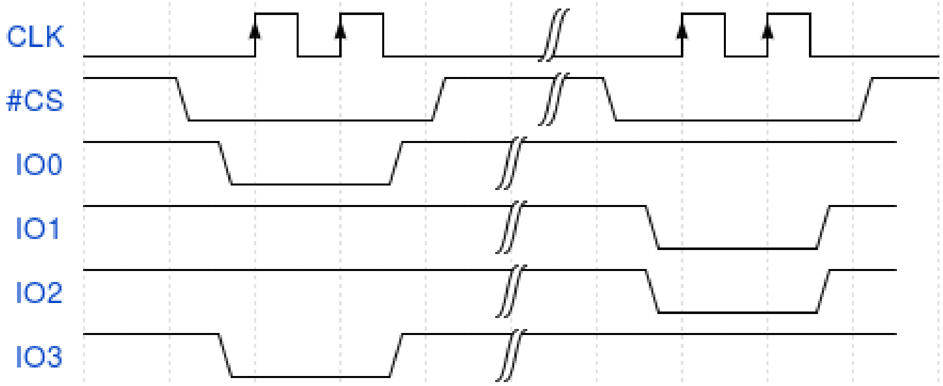
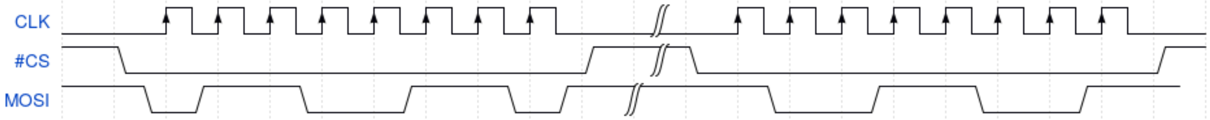


Figure 2-2. Reset Command Sequence in SPI 1-1-1



2.4.2.2 Probing the Read Parameters

The ROM Code relies on two mechanisms to probe any (Q)SPI NOR Flash memory connected to its QSPI controllers. First, the ROM code tries to read the Serial Flash Discoverable Parameters (SFDP) tables, hard-coded inside a ROM area of QSPI NOR Flash memories compliant with the JEDEC JESD216 specification, to learn all the required parameters to read data from those memories.

If and only if the ROM code fails to read valid SFDP tables, then it falls back into another hard-coded table stored inside the ROM code itself. To limit the size of this table in the ROM code, there is only one set of read parameters for each of the following JEDEC Manufacturer IDs:

- 01h (Spansion/Cypress)
- 20h (Micron)
- C2h (Macronix)
- EFh (Winbond)
- Others

Note: Unlike MRL B, the ROM code of SAMA5D2 MRL C no longer uses the SPI 4-4-4 protocol with Micron QSPI NOR Flash memories; only SPI 1-y-z protocols are used with all memory manufacturers.

More details about read parameters can be found in the SAMA5D2 data sheet, section “QSPI NOR Flash Boot for MRL C”.

2.4.2.3 Setting the Quad Enable (QE) Bit

For almost all memory manufacturers, the QE bit is non-volatile and must be set before performing any SPI command that requires the 4 I/O lines. This is the only persistent setting that the ROM code may change in the internal registers of the QSPI NOR Flash memory. All other settings are kept unchanged.

The procedure to set this QE bit is manufacturer-specific and may also change between different memory models of the same manufacturer.

Again, the ROM code first checks the SFDP tables to find out the right procedure. If no SFDP table is found, then the ROM code looks up in its own hard-coded table to get the procedure to be executed.

More precisely, the ROM code reads bits[22:20] in DWORD15 from the Basic Flash Parameter Table (refer to JEDEC JESD216B specification) to select and then execute the relevant procedure, if any, to set the QE bit.

2.4.2.4 Known Limitations

Values 001b and 100b for bits[22:20] in DWORD15 of the Basic Flash Parameter Table are not correctly supported by the ROM code SAMA5D2 MRL C. Consequently, booting from memories using one of the above values in their SFDP tables is highly likely to fail.

⚠WARNING This issue prevents the ROM code from booting with all Winbond memories that have been tested in Microchip.

Refer to the memory datasheet for the value to be programmed by the memory manufacturer in the SFDP tables.

2.4.2.5 Supported QSPI Memories by Manufacturer (MRL C)

Table 2-1. Tested and Supported QSPI NOR Flash Memories by SAMA5D2 MRL C (non-exhaustive)

Manufacturer	Memories
Microchip (SST)	SST26VF080B SST26VF016B SST26VF032B SST26VF032BA SST26VF064B
Micron	N25Q128A13 N25Q256A13 N25Q512A13 MT25QL01G

Manufacturer	Memories
Macronix	MX25V4035FM2I MX25V8035FM2I MX25V1635FM2I MX25L3233FM2I-08G MX25L3273FM2I-08G MX25L6433FM2I-08G MX25L6473FM2I-08G MX25L12835FM2I-10G MX25L12845GMI-08G MX25L12873GM2I-08G MX25L25635MZ2I-10G MX25L25645GMI-08G MX25L25673GMI-08G MX25L51245GMI-08G MX25L51245GMI-10G MX66L1G45GMI-08G
Spansion/Cypress	S25FL127 (normal boot only; XIP fails) S25FL164 S25FL512

3. Revision History

3.1 Rev. A - 08/2018

First issue.

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-5224-3474-0

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/
support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Australia - Sydney
Tel: 61-2-9868-6733

China - Beijing
Tel: 86-10-8569-7000

China - Chengdu
Tel: 86-28-8665-5511

China - Chongqing
Tel: 86-23-8980-9588

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115

China - Hong Kong SAR
Tel: 852-2943-5100

China - Nanjing
Tel: 86-25-8473-2460

China - Qingdao
Tel: 86-532-8502-7355

China - Shanghai
Tel: 86-21-3326-8000

China - Shenyang
Tel: 86-24-2334-2829

China - Shenzhen
Tel: 86-755-8864-2200

China - Suzhou
Tel: 86-186-6233-1526

China - Wuhan
Tel: 86-27-5980-5300

China - Xian
Tel: 86-29-8833-7252

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444

India - New Delhi
Tel: 91-11-4160-8631

India - Pune
Tel: 91-20-4121-0141

Japan - Osaka
Tel: 81-6-6152-7160

Japan - Tokyo
Tel: 81-3-6880- 3770

Korea - Daegu
Tel: 82-53-744-4301

Korea - Seoul
Tel: 82-2-554-7200

Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

Malaysia - Penang
Tel: 60-4-227-8870

Philippines - Manila
Tel: 63-2-634-9065

Singapore
Tel: 65-6334-8870

Taiwan - Hsin Chu
Tel: 886-3-577-8366

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600

Thailand - Bangkok
Tel: 66-2-694-1351

Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-67-3636

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra’anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-7289-7561

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820