AN4971

Booting from External Non-Volatile Memory (NVM) on SAM9X7 MPUs

Introduction

This document describes the boot process of the SAM9X7 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 process.

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 SAM9X7 in the system through a USB, RS-232 or JTAG link. The tool suite is available on the Microchip web site, on the product page.

Secure SAM-BA Cipher, available on request, is used to prepare ciphered keys and application files for programming and to configure the Secure Boot mode on the SAM9X7, 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 SAM9X7 MPU.

Reference Documents

Document Type	Document Title	Literature Number	Available
Data Sheet	SAM9X7 Series	DS60001813	www.microchip.com

© 2023 Microchip Technology Inc. and its subsidiaries

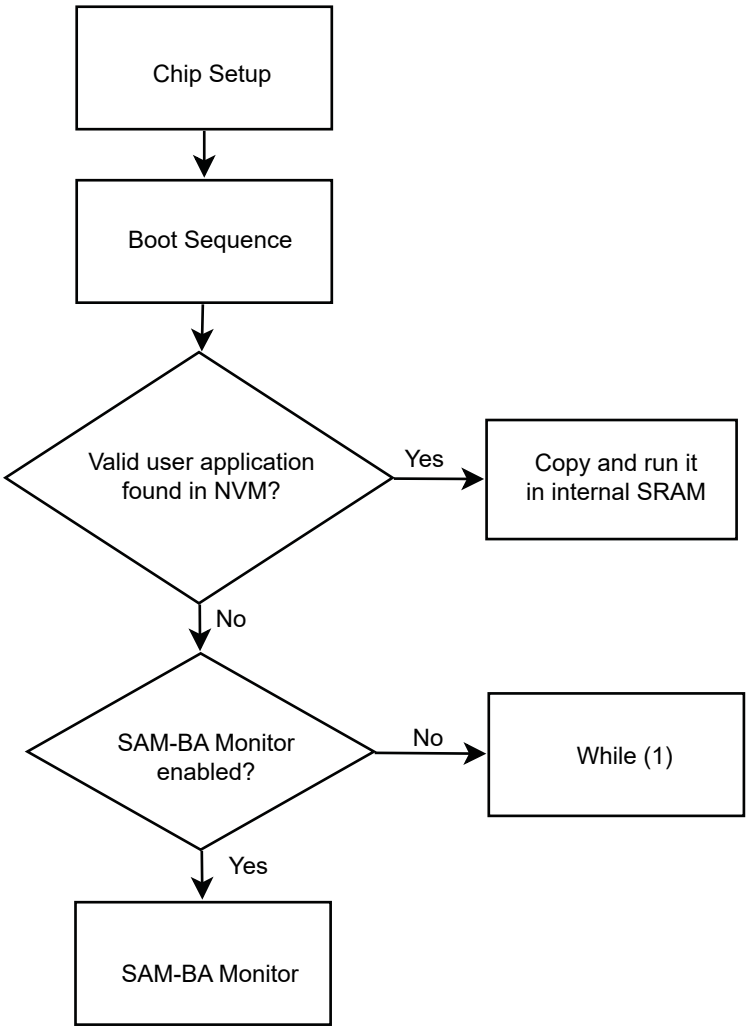
1. Role of the ROM Code

The ROM code (or Boot ROM) is stored in on-chip mask ROM and executes on power-on or after a Reset. It is 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. 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 to execute the user application.

The user application should be linked so that its entry point is at the very beginning of the internal SRAM. Nevertheless, just before jumping to the user application, the ROM code also remaps the internal SRAM at address 0x0. Thus when the user application places its Arm® exception vector table at the beginning of the internal SRAM, the vectors are also seen at 0x0 by the Arm core when it needs to access them.

In the Arm9™ architecture, the 6th exception vector is reserved and the ROM code uses this 32-bit data to store the size of the user application. The ROM code fetches this value to know exactly how many bytes it should transfer from the external NVM, optimizing boot time. 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



1.1 Boot Sequence

For SAM9X7, the boot sequence is:

1. SDMMC0 IOSET1
2. SDMMC1 IOSET1
3. QSPI IOSET1
4. SPI5 IOSET1
5. NAND IOSET1

The user can configure a specific boot sequence tailored for the system by writing a Boot Configuration Packet in the One Time Programmable (OTP) memory. Refer to the product data sheet, section “Boot Configuration” 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. Refer to ROM Code Process Flow.

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

The SAM-BA tool is a software program, running on a PC under Windows® or Linux®, which connects 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 tool, Secure SAM-BA Cipher, is distributed under Non-Disclosure Agreement (NDA) only and is used to prepare files to be used with the Secure Boot mode of the ROM code.

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. Once the Secure Boot mode is enabled, the ROM code expects the user application in the external NVM to be ciphered and signed.

The user application is ciphered with the AES-256-CBC algorithm and signed with either AES-256-CMAC or RSA algorithm, using Secure SAM-BA Cipher to guarantee its integrity and authenticity.

The customer key is a shared secret between the customer and the microprocessor, and is written once in the OTP memory with the help of the SAM-BA tool.

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 authenticated and deciphered in the internal SRAM and before executing it, the ROM code forbids any further access to the customer key until the next Reset. This way the customer key cannot be extracted by any software running in the SoC.

To prepare the provisioning of the customer key during manufacturing, this key must be 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 microprocessor-based design.

Then the programming of the customer boards is done by the third party manufacturer with the help of the SAM-BA tool. Only the ROM code is able to decrypt and authenticate the customer key received from the SAM-BA tool. Thus 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.

© 2023 Microchip Technology Inc. and its subsidiaries

2. Supported External Non-Volatile Memories (NVM)

2.1 SDCard/e.MMC Boot

Boot may be done from SDCard or e.MMC memories connected to SDMMC0 or SDMMC1. Though SDMMC0/ SDMMC1 support 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 an e.MMC boot partition is enabled. If so, the maximum bootstrap size of the enabled boot partition is 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.

⚠WARNING Implementing SDCard/e.MMC boot requires particular attention to the connection of the Card Detect pin. For information, refer to the section “SDCard/e.MMC Boot” of the data sheet.

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.

The correct PMECC parameters are indicated to the ROM code by writing a specific header at the beginning of the first page of the NAND Flash, just before the bootstrap. 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 SAM9X7 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 any FLEXCOM interface that supports SPI, and if the SPI NOR Flash memories are compatible with either AT25, AT26 Serial Flash or AT45 DataFlash memories. Refer to the product 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 QSPI.

Important: QSPI NAND Flash memories are not supported.

2.4.1 Software Reset of the QSPI NOR Flash Memory

QSPI limitations of the ROM code 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

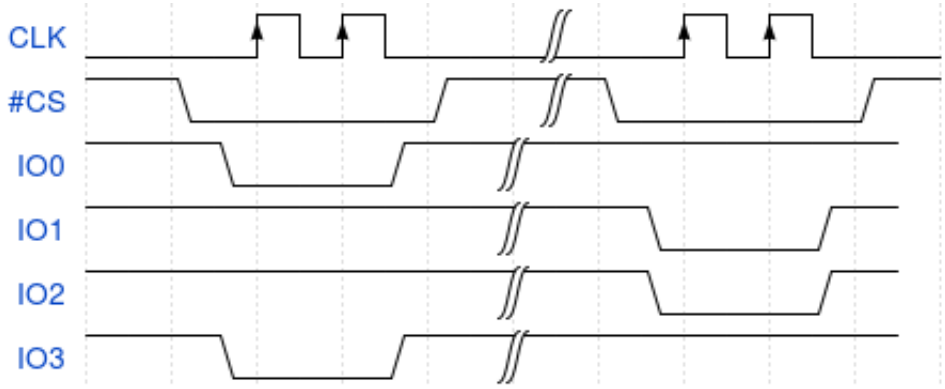
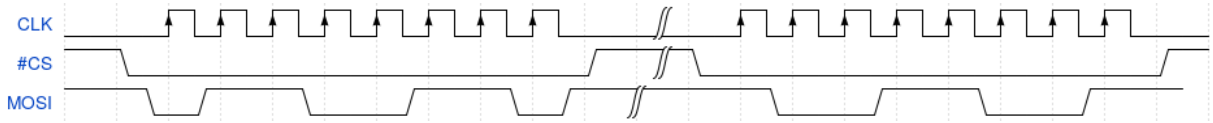


Figure 2-2. Reset Command Sequence in SPI 1-1-1



2.4.2 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

2.4.3 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.

© 2023 Microchip Technology Inc. and its subsidiaries

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.

2.4.4 Supported QSPI Memories by Manufacturer

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

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

© 2023 Microchip Technology Inc.
and its subsidiaries

3. Revision History

3.1 Rev. A - 03/2023

First issue.

Table of Contents

© 2023 Microchip Technology Inc.
and its subsidiaries

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **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 (FAQs), technical support requests, online discussion groups, Microchip design partner 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

Product Change Notification Service

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

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

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

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded

© 2023 Microchip Technology Inc. and its subsidiaries

by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". 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 ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

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, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, and ZL 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, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, 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.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks 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.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-2241-3

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: 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	**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	**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	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 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: 49-7131-72400 **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: 47-72884388 **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

© 2023 Microchip Technology Inc.
and its subsidiaries