AN2747

Robustness on tinyAVR® 0- and 1-series and megaAVR® 0-series

Introduction

Author: Per Andreas Gulbrandsen, Øyvind A. Sandberg, Microchip Technology Inc.

In the *IEEE Standard 610.12-1990 Glossary of Software Engineering Terminology* robustness is defined as *"The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions."* This document is a guide to peripherals available in tinyAVR® 0- and 1-series and megaAVR® 0-series that can be used in robustness applications.

Table of Contents

1. Relevant Devices

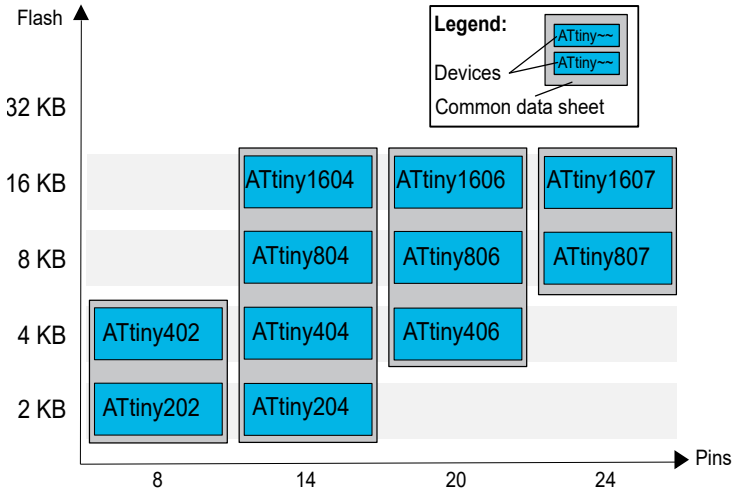
This chapter lists the relevant devices for this document.

1.1 tinyAVR® 0-series

The figure below shows the tinyAVR® 0-series devices, laying out pin count variants and memory sizes:

- Vertical migration upwards is possible without code modification, as these devices are pin-compatible and provide the same or more features
- Horizontal migration to the left reduces the pin count and, therefore, the available features

Figure 1-1. tinyAVR® 0-series Overview



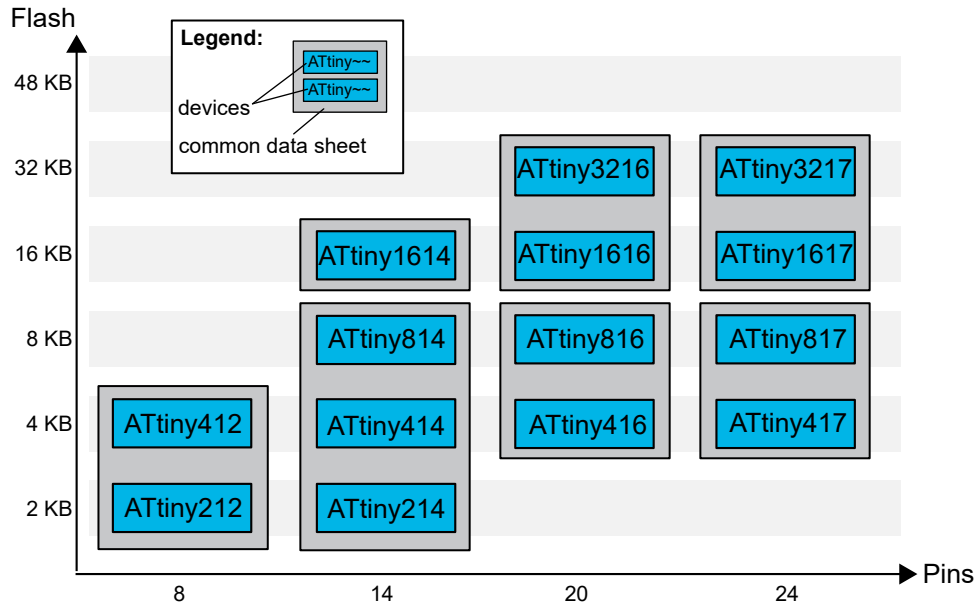
Devices with different Flash memory sizes typically also have different SRAM and EEPROM.

1.2 tinyAVR® 1-series

The following figure shows the tinyAVR 1-series devices, laying out pin count variants and memory sizes:

- Vertical migration upwards is possible without code modification, as these devices are pin-compatible and provide the same or more features. Downward migration may require code modification due to fewer available instances of some peripherals.
- Horizontal migration to the left reduces the pin count and, therefore, the available features

Figure 1-2. tinyAVR® 1-series Overview



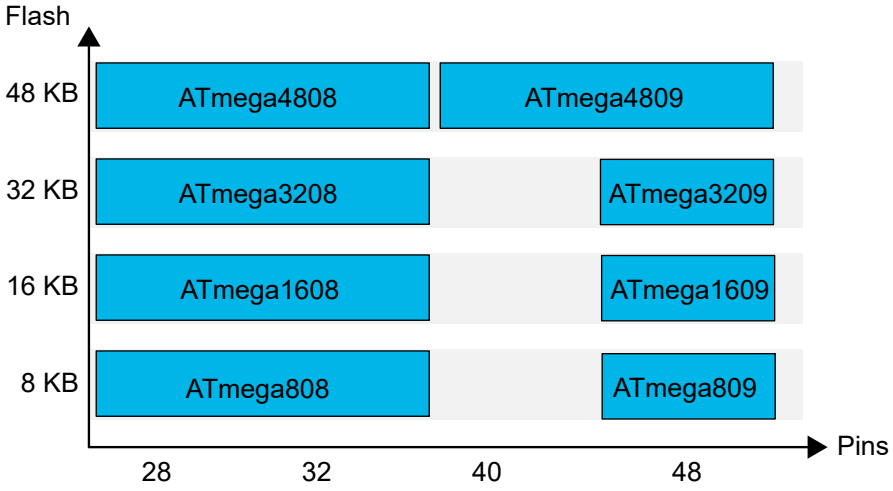
Devices with different Flash memory sizes typically also have different SRAM and EEPROM.

1.3 megaAVR® 0-series

The figure below shows the megaAVR® 0-series devices, laying out pin count variants and memory sizes:

- Vertical migration is possible without code modification, as these devices are fully pin and feature compatible
- Horizontal migration to the left reduces the pin count and, therefore, the available features

Figure 1-3. megaAVR® 0-series Overview



Devices with different Flash memory sizes typically also have different SRAM and EEPROM.

2. Power-on Reset

The Power-on Reset (POR) circuit is a non-configurable circuit that ensures the device is reset when powered on, with what is called a Power-on Reset. During POR, all logic is reset, and all registers are initialized, including registers that are loaded from fuses. This procedure ensures that the MCU starts execution in a known good state.

The POR circuit is always active and works by comparing the supply voltage with fixed threshold levels, either rising or falling. These threshold levels are not configurable, unlike the BOD level. See section 3. Brown-out Detector.

Both POR rising threshold level and POR falling threshold level are specified in the electrical characteristics section of the Relevant Devices data sheet.

When the supply voltage is below the rising threshold, the POR circuit will assert the internal Reset. When the supply voltage rises above the threshold, the device will be allowed to start-up.

In the case of a power dip, the POR circuit compares the supply voltage to a POR falling threshold level. If the supply voltage dips below this threshold, the internal Reset will be reasserted, until the supply voltage again rises above the POR rising threshold level.

If the device is reset by POR, the POR flag in the Reset Flag (RSTCTRL.RSTFR) register is set. After a POR, only the POR flag is set, all other flags are cleared.

3. Brown-out Detector

For the CPU to successfully decode and execute instructions, the supplied voltage must always stay above the minimum voltage level. This level is defined by the chosen operating frequency. For example, an operating frequency of 10 MHz on the Relevant Devices, an operating voltage of minimum 2.7V, must be supplied. If the voltage drops below this threshold, unexpected behavior of the microcontroller (MCU) might occur. This can include incorrect execution of instructions, corruption of CPU registers, Flash corruption, and unexpected toggling of pins. Also, it can cause logic to latch up, possibly entering into incorrect states.

To avoid the above issues, a Brown-out Detector (BOD) can be used. The Relevant Devices includes an on-board, configurable BOD, which monitors the power supply and compares the voltage with a programmable brown-out threshold level. When the BOD detects that the supply voltage crosses the configured threshold, it will assert the internal Reset. As long as the supply voltage remains below the configured threshold level, the device will be kept in Reset. When the supply voltage is above the threshold level, and normal operation can safely continue, the BOD will deassert the internal Reset, allowing the device to execute instructions.

After a Reset, the BOD settings are loaded from fuses. There are two fuses to control the BOD functionality, which are found in the BOD Configuration (BODCFG) under Fuses in the device data sheet.

The first fuse, ACTIVE, defines the operation mode while in Active or in Idle sleep mode. These bits can not be altered by software.

The second fuse, SLEEP, defines the operation mode while in Standby or Power-down sleep mode. These bits may be altered by software and are under the Configuration Change Protection (CCP).

The ACTIVE and SLEEP fuses can be configured in the following ways:

- *Disabled mode* - BOD is deactivated
- *Enabled mode* - means that BOD is continuously active
- *Sampled mode* - BOD is activated briefly at a given period to check the supply voltage level. Frequency is set to either 125 Hz or 1 kHz in Sample Frequency (BODCFG.SAMPFREQ) fuse

Also, ACTIVE has a fourth option:

- *Enabled with wake-up halted until BOD is ready* - BOD is not active during sleep. On wake-up, the code execution is halted until BOD is ready. This ensures the correct supply voltage whenever the code is executed. The wake-up time may be extended.

Sample Frequency (SAMPLEFREQ) and BOD Level (LVL) are also found in BODCFG. These control how the BOD behaves.

BOD Levels

The BOD compares the supply voltage to a threshold level. This threshold is programmable, and the user can select from 8 different levels. Table 3-1 shows the BOD levels from the ATtiny3217 data sheet. Always check the Relevant Devices data sheet for correct BOD levels.

Table 3-1. BOD Threshold Level Examples

Name	Description
BODLEVEL0	1.80V
BODLEVEL2	2.60V
BODLEVEL7	4.30V

When setting the BOD level, several things come into consideration. As already mentioned, the BOD can protect the system from an unsafe operation. Also, the BOD can be used to ensure voltage levels, e.g., when using the ADC. If the ADC is set to sample using the 4.3V internal reference, and the supply voltage drops below this level, the ADC results will be incorrect.

If the BOD is unused, it will be set to the minimum level to ensure safe operation during an internal Reset and chip erase.

3.1 Voltage Level Monitor

The Voltage Level Monitor (VLM) acts as an early warning and generates an interrupt request if the supply voltage is about to drop below a given threshold level. This can allow the system to do a safe shutdown.

Being a part of the BOD peripheral, the VLM threshold level can be configured to either 5%, 15% or 25% above the BOD level. The VLM follows BOD functionality. If the BOD is in Sampled mode, the VLM will also be sampled. If the BOD is disabled, the VLM is disabled.

The VLM interrupt can be triggered when the supply voltage crosses from above, from below, or either direction of the threshold level.

4. Watchdog Timer

Many issues can cause a system to enter an illegal or frozen state, e.g., software bugs or electrical noise. One safety measure available on the Relevant Devices is the Watchdog Timer (WDT). This is a timer that runs independently from the rest of the system, with a separate clock source. When the timer overflows, it will cause a Reset. The system firmware must periodically clear the WDT using the dedicated instruction Watchdog Timer Reset (`WDR`). If the firmware is not able to do so, e.g., due to a system hang or run-away code, the system will be Reset.

Normal mode

In Normal mode, the watchdog counts from 0 to the MAX value and can be cleared at any time. The period in Normal mode can be configured with a duration from 8 ms to 8s.

Window mode

For increased robustness, Window mode is available. In Window mode, both a closed and an open window are configured, with the closed window being at the start of the period. While in the closed window, clearing the WDT is an illegal operation, resulting in a Reset. Once the closed window is over, the open window starts and the WDT can now be cleared. Using Window mode puts more requirements on the firmware, as it must clear the watchdog in the open window only. Both windows can be configured with a duration of 8 ms to 8s. This gives a total WDT period of 16 ms to 16s.

The WDT period and window timeouts can be configured by fuses so that it is active immediately after Reset. Should there be any issue with the firmware, causing it to not start properly, the WDT will reset the system. The WDT will start to count from 0 after Reset, regardless of the Reset source.

As one of the goals of implementing a watchdog timer is to be able to recover from the run-away code, there are a few things the software engineer may consider. The run-away code does not influence the execution of an interrupt. Any interrupt vector will be correctly loaded, even when the system for some reason is executing the wrong code. Therefore, do not clear the WDT from an interrupt handler. Also, try to limit the amount of `WDR` instructions. If clearing the WDT is done in many parts of the firmware, it becomes more likely that one of these is executed when the run-away code is being executed. Ideally, only one `WDR` instruction may be implemented. This can be hard to achieve, but it is important to try to limit the amount of `WDR` instructions. Using the Window mode can also help catch erroneously executed `WDR` instructions.

5. CRCSCAN

A Cyclic Redundancy Check (CRC) creates a checksum for a block of data, enabling error detection of the data block. The Relevant Devices feature the CRCSCAN peripheral, which can check a Flash section and compare it to a checksum stored at the end of the section. If the Flash section is accidentally changed, i.e., because of corruption or an unintended write, the CRCSCAN will detect this and signal to the CPU that Flash has been corrupted.

In a bootloader application, CRCSCAN can be used to verify the application image before starting execution. This to make sure that corrupted software is not executed, which could have catastrophic consequences. If the check fails, the bootloader can either choose not to start the application, it can do a firmware update, or it can signal the error to an external system.

CRCSCAN can be run at start-up, or specific intervals controlled by the application. When running at start-up, the Flash is checked for errors before any instruction is executed. This allows the integrity of the application to be verified before execution. CRCSCAN on start-up is configured using fuses.

When CRCSCAN is controlled by the application, it can be started by register access. When started, the CPU is halted while the check is being done, as CRCSCAN has priority access to Flash, thus blocking the CPU.

For more information, refer to the *CRCSCAN on tinyAVR® 0- and 1-series and megaAVR® 0-series* application note.

6. Class B

Modern appliances are mostly electronically controlled. Electronic controls enable higher efficiencies, additional functionality, and improved user experience. But what happens if something goes wrong? IEC 60730 addresses the safety of electronic controls in appliances. This standard is also referred to by other standards for safety-critical devices, for example, IEC 60335. Currently, IEC 60730 is mandatory for appliances sold in Europe.

IEC 60730 Annex H defines three classes of control software for appliances:

- Class A - control functions that are not intended to be relied upon for the safety of the equipment
- Class B - software that includes code intended to prevent hazards if a fault, other than a software fault, occurs in the appliance
- Class C - software that includes code intended to prevent hazards without the use of other protective devices

For an appliance to comply with the Class B requirements, the control software must detect and handle faults for system components. For a customer wishing to certify a product following Class B requirements, Microchip offers a Class B library for tinyAVR® 1-series. This library implements the tests needed to comply with Class B and can reduce development time and certification cost.

Tests are done on CPU registers, program counter, frequency, CRC, interrupt handling and execution, clock, SRAM, Flash, EEPROM, and peripherals such as ADC, DAC, and WDT.

For more information, refer to *Guide to IEC 60730 Class B Compliance with tinyAVR® 1-series*.

7. Configuration Change Protection

System critical registers are protected from accidental modification, and Flash self-programming is protected from accidental execution. This is handled globally by the Configuration Change Protection (CPU.CCP) register. Execution of either of these actions is only possible after a signature has been written to the CCP register. After writing the correct signature to the CCP register, the desired action must be executed within four instructions. Interrupts are kept pending during these four cycles.

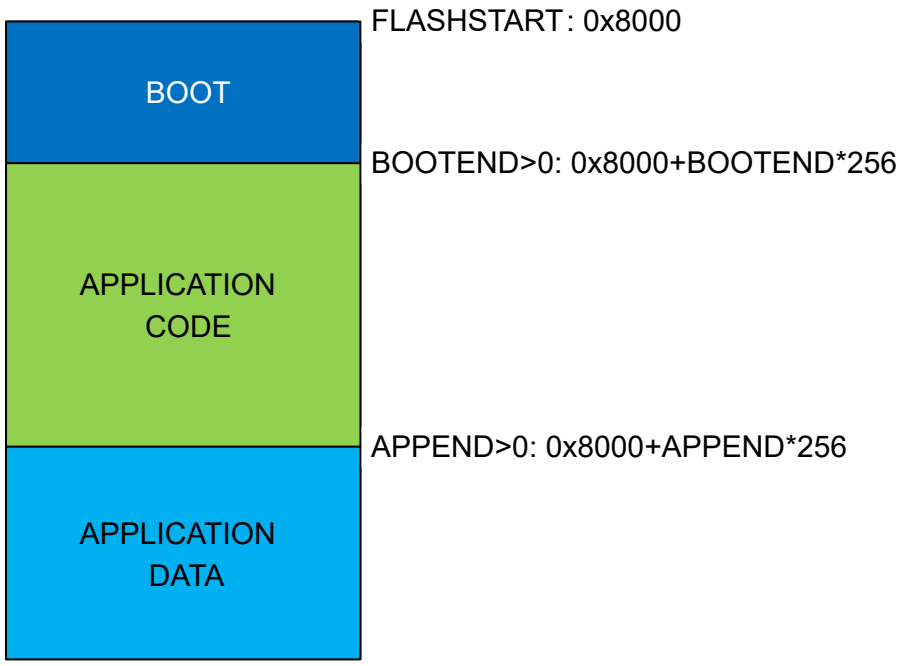
Refer to the CPU section in the Relevant Devices data sheet for details on CCP.

8. Flash Sections

Flash of the Relevant Devices can be split into three separate sections: BOOT, application code (APPCODE) and application data (APPDATA). This scheme allows for the protection and safe storage of several individual segments of code or data. The granularity of the division is 256 bytes.

The size of the three sections is set using the fuses Boot Section End (BOOTEND) and Application Code Section End (APPEND). BOOTEND determines the size of the BOOT. APPEND determines the size of the APPCODE. APPCODE will be placed immediately after the BOOT. The remaining pages will be part of APPDATA, placed immediately after APPCODE. If both fuses are set to zero, all pages are allocated to the BOOT. This is the normal procedure if only an application is written to Flash, with no bootloader.

Figure 8-1. Flash Sections



If FUSE.BOOTEND is written to 0x04 and FUSE.APPEND is written to 0x08, the first 4*256 bytes will be BOOT, the next 4*256 bytes will be APPCODE, and the remaining Flash will be APPDATA.

To protect the data in the three sections, directional write protection is implemented:

- Code in the BOOT section can write to APPCODE and APPDATA
- Code in APPCODE can write to APPDATA
- Code in APPDATA cannot write to Flash or EEPROM

In addition to the directional write protection, two register bits can be used to increase restrictions.

By writing a `1` to the Application Code Section Write Protection (APCWP) bit, the application code section is protected from further writes. The bit can be found in the Control B (CTRLB) register of the Nonvolatile Memory Controller (NVMCTRL) peripheral. This bit is cleared on Reset.

As the BOOT section can never be written by the CPU, there is no need to protect BOOT from writes in the same manner. But by writing a `1` to the Boot Section Lock (BOOTLOCK) bit in CTRLB register of the NVMCTRL peripheral, reading and executing code from BOOT can be prevented. This bit is cleared on Reset.

Refer to the Nonvolatile Memory Controller (NVMCTRL) chapter in the Relevant Devices data sheet for more details.

9. Fuses

Fuses are part of the nonvolatile memory and are used to configure system settings such as clock source, start-up time, Flash sections, etc. Fuses can be read by both the CPU and an external programmer, but only programmed or cleared by an external programmer. Some registers are reset to a value stored in the fuses, such as oscillator calibration. These values are written at the end of the start-up sequence. Thus, when such a fuse is changed, the device must be reset before the change takes effect.

Fuses for peripheral configuration include:

- Watchdog Timer: Used to set the WDT window and timeout period upon start-up, thus not requiring any code execution to operate.
- Brown-out Detector: Used to set the BOD level, sample frequency, Active and Standby operating mode, thus not requiring any code execution to operate.
- *16/20 MHz Oscillator*: Configures whether the operating frequency should be 16 or 20 MHz. It is also possible to lock the calibration registers after they are loaded with factory calibration values.
- Timer/Counter D: Used to enable or disable TCD output pins, and also to set the default state of the pins. This fuse is only available for devices in the tinyAVR® 1-series.
- *System Configuration 0*: Used to configure the CRCSCAN to run on start-up, and to select which Flash section to check.
- *System Configuration 1*: Used to configure additional start-up time of the device.
- Application Code End: Used to configure the size of the application code section.
- Boot End: Used to configure the size of the boot section.
- *Lockbits*: Used to lock the device and prevent an external programmer from accessing the fuses, Flash, SRAM and EEPROM. Regular memory access from within the application still is enabled. A chip erase must be executed to unlock a device.

Using fuses to set up, e.g., a WDT before any code is executed increases the robustness of the system. This because corrupt Flash could cause a software-driven configuration of the WDT to fail. Imagine that the instruction enabling the WDT is corrupt and is not properly executed. The result is a system that misbehaves, and the mechanisms to detect erroneous behavior is disabled. Therefore, enabling security features using fuses is an advantage.

Enabling CRCSCAN using fuses allows the Flash to be scanned for errors before any instruction has been fetched from Flash.

For more information, refer to the Fuses sub-section in the Memories chapter in the Relevant Devices data sheet.

10. Events and Fault Handling

This section is relevant only for devices in the tinyAVR® 1-series. The Timer/Counter type D (TCD) is a timer/counter specifically designed for controlling power applications like driving LEDs, motor control, H-Bridge and power converters. An important safety feature of TCD is the built-in fault handler. The fault handler allows the output of TCD to be clamped to predefined levels upon a fault. The fault is an incoming event, and some other internal or external peripheral must be present to discover the condition.

Imagine the TCD driving an motor for a fan. The Analog Comparator (AC) is also connected to the fan and monitors the current consumption. If the current consumption rises above a predefined threshold, e.g., due to something being stuck in the fan, the AC sends an event to the TCD. Upon receiving the event, TCD immediately clamps all outputs to a predefined level, and the motor stops. This way, the motor is stopped safely before overheating or destroying the object that caused the blockage.

When using an external circuit instead of an internal peripheral, the event is generated by an edge or change in the level of the pin connected to the external circuit. Again, this event is sent to the TCD, which immediately clamps all output to a predefined state.

The event is sent via the Event System (EVSYS). The EVSYS enables direct peripheral to peripheral signaling. One peripheral (Event Generator) can signal to one or several other peripherals (Event Users), without using the CPU.

All parts of the described examples are core independent (CIP), meaning that even if the CPU is deadlocked, this safety feature will work like intended.

11. Revision History

Doc. Rev.	Date	Comments
C	11/2019	Changed title to reflect that the application note is also relevant for tinyAVR® 0-series and megaAVR® 0-series. Removed unsupported BOD levels in Table 3-1. Clarified tinyAVR® 1-series specific features in the Class B, Fuses and Events and Fault Handling section.
B	10/2018	The chapter on relevant devices has been updated to include 8/16 KB megaAVR 0-series devices.
A	06/2018	Initial document release

The Microchip Website

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

APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, FlashTec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, Vite, WinPath, 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, BlueSky, 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, 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.

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.

ISBN: 978-1-5224-5260-7

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit http://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: http://www.microchip.com/support Web Address: http://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: 45-4450-2828 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: 49-7131-72400 **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