CodeGuard™ Security: Protecting Intellectual Property in Collaborative System Designs

Author: *Rishi Vasuki*
Microchip Technology Inc.

EXECUTIVE SUMMARY

Microchip's CodeGuard™ Security enables multiple parties to more securely share resources (memory, interrupts and peripherals) on a single chip. Intellectual Property (IP) Vendors, Original Design/Equipment Manufacturers (ODM/OEM) and Value-Added Resellers (VAR) now have an opportunity to reap the following benefits using these advanced on-chip security features:

- System cost reduction
- Component reduction and associated benefits to inventory management
- Decreased risk of losing IP to unqualified partners
- Increased security during program distribution and Flash memory update

CodeGuard Security is a turnkey solution with basic, intermediate and advanced implementations on Microchip's compatible line of 16-bit Flash memory-based PIC24 Microcontrollers (MCU) and dsPIC® Digital Signal Controllers (DSC).

INTRODUCTION

Microchip's CodeGuard Security represents unique advancements in the realm of embedded firmware security. This white paper describes CodeGuard Security and discusses application scenarios that will find these features beneficial. The description of the salient features of CodeGuard Security is complemented by a discussion on available tools and software useful to the design engineering community.

WHO BENEFITS FROM CodeGuard Security?

Software Intellectual Property (IP) vendors, OEMs, Programming Centers and Contract Manufacturers of embedded systems benefit from CodeGuard Security. If your organization uses a Code Protection feature available on MCUs, DSCs or DSPs, CodeGuard Security may be useful to you in collaborating with your design partners to reduce your system cost and reduce the risk of IP loss.

WHO SHOULD READ THIS WHITE PAPER?

This document provides guidance to design engineers, product development managers, as well as costing, component and procurement specialists. The following guidelines may prove useful for faster readability. We recommend:

- Product Development and Operations Managers read **Section "Protecting Embedded Intellectual Property (IP)"** and **Section "Process Flow: From Software Development to Production"**
- Costing, Component and Procurement Specialists read **Section "Protecting Embedded Intellectual Property (IP)"**, **Section "CodeGuard Security: Featured Products and Availability"** and **Section "Process Flow: From Software Development to Production"**
- Design Engineers read the entire document

PROTECTING EMBEDDED INTELLECTUAL PROPERTY (IP)

Protecting a company's IP is one of the highest priorities in a competitive marketplace. In embedded applications, OEMs, design houses and software vendors face some critical issues in trying to protect their IP while collaborating on system designs. These issues are listed below:

1. IP protection measures increase system cost for OEMs and VARs
2. Software vendors and design houses risk losing IP to unqualified partners
3. Insufficient on-chip support for secure program distribution and Flash memory update

We examine each of these issues in detail and describe how CodeGuard Security provides a solution.

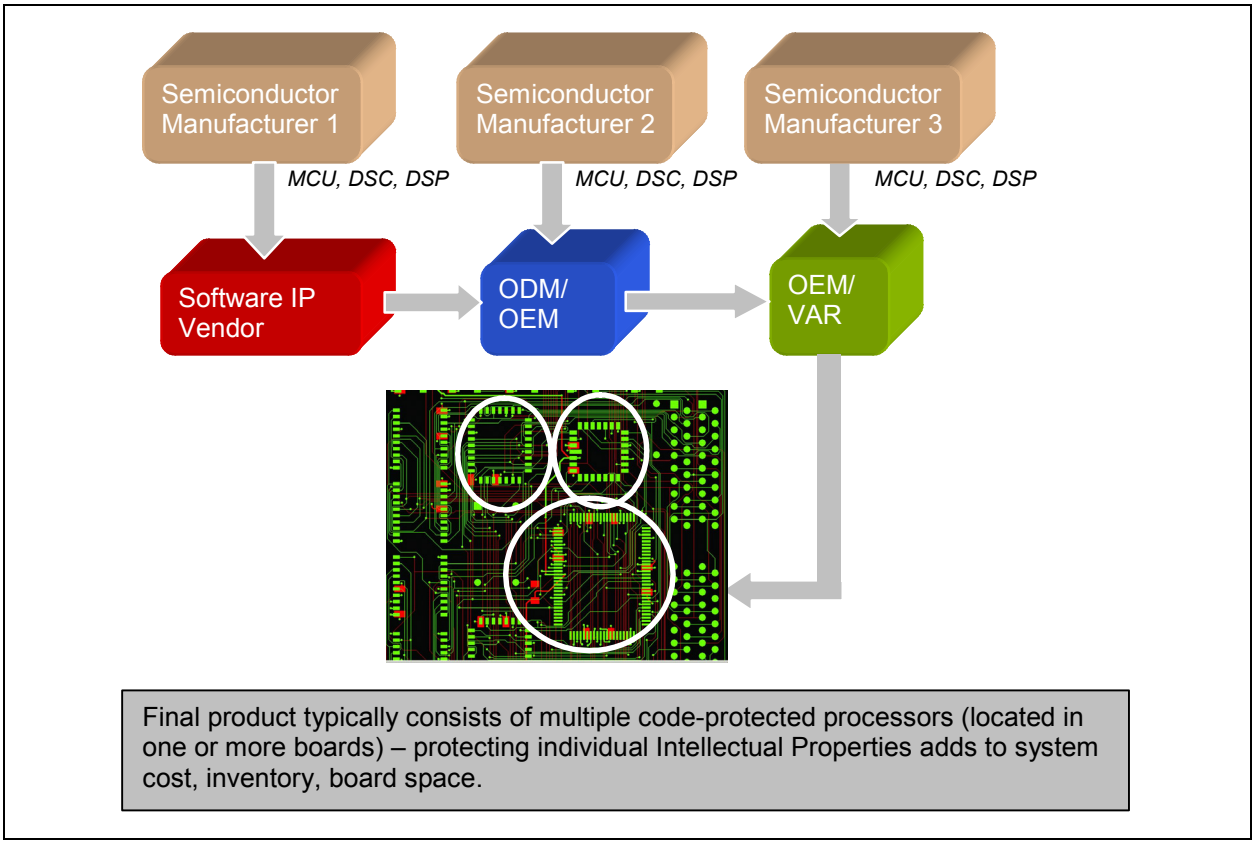
ISSUE: PROTECTING IP INCREASES SYSTEM COST

In today's business environment, Original Design/ Equipment Manufacturers (ODM/OEM), Software IP Vendors and Value Added Resellers (VAR) increasingly engage in collaborative supplier-buyer relationships while developing new products. Each of these parties may own Intellectual Property (IP) they would want to protect. This IP is increasingly in the form of firmware or program resident in the Flash memory of embedded processors such as Microcontrollers (MCU), Digital Signal Processors (DSP) or Digital Signal Controllers (DSC). Having had their IP stolen in the past, today's IP vendors and OEMs often resort to using on-chip memory or code protection features to disallow competitors from copying their firmware.

Given that each vendor or OEM in the supply chain would like to protect their own IP, often the final product sold to the end customer may contain two to three embedded microcontrollers, each protecting the firmware of one of these parties. Essentially, each vendor deems their own IP important enough that they find a home for it in a dedicated code-protected microcontroller. From a system cost perspective, this end product is inefficient. From a component procurement (purchasing) specialist's perspective, managing inventories and lead times of three microprocessors is quite a challenge. From a system designer's perspective, there is a large opportunity for system integration into one microcontroller. This is exactly what the CodeGuard Security facilitates.

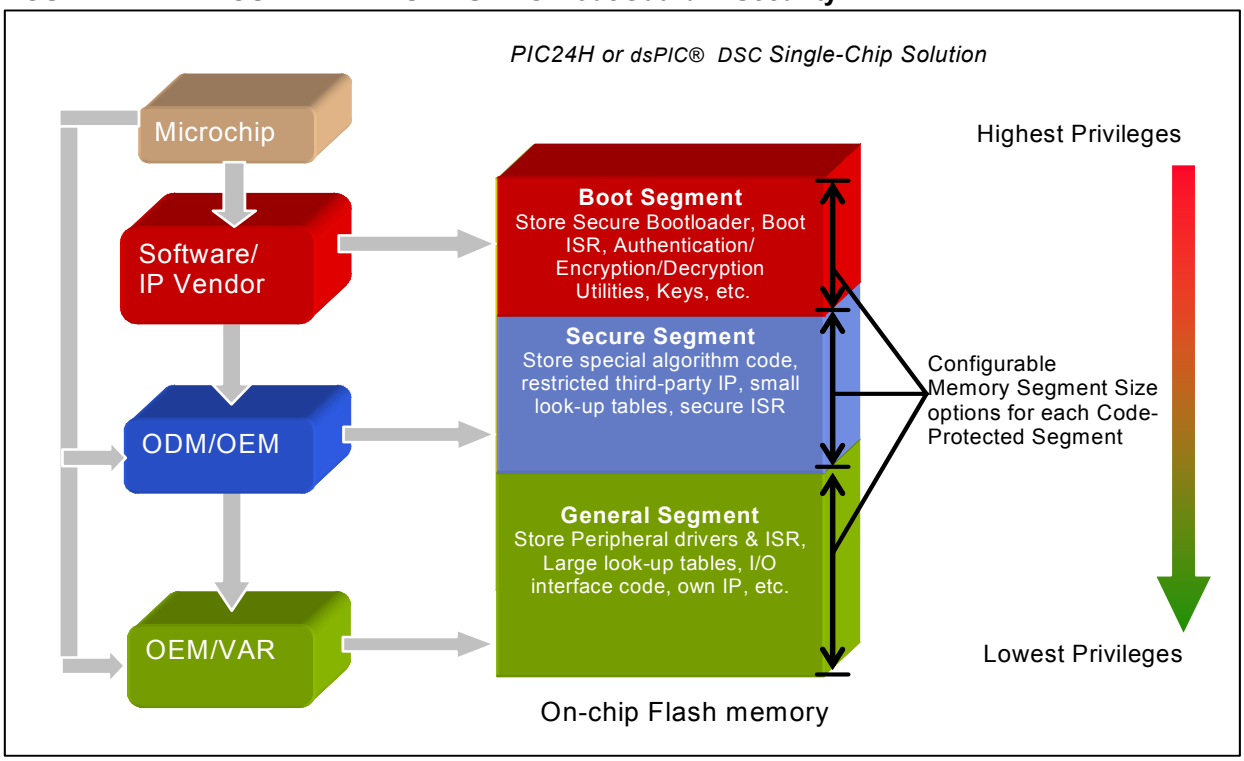
Figure 1 shows a block diagram describing a generic collaborative embedded system design model. Derivatives of this model are in use today. Figure 1 highlights the cost inefficiencies introduced by the lack of an appropriate MCU or DSC solution.

FIGURE 1: INCREASED SYSTEM COST DUE TO IP PROTECTION IN COLLABORATIVE DESIGNS



SOLUTION: SYSTEM COST REDUCTION
USING CodeGuard Security

FIGURE 2: COST DECREASE DUE TO CodeGuard™ Security



Microchip's CodeGuard Security offers a system cost reduction by enabling multiple parties (software vendors, OEMs and their partners) to securely share a single chip's resources as shown in Figure 2. Thus, multiple processors may be integrated into a single 16-bit MCU or DSC. Final products may then be offered to customers at more attractive costs while decreasing component count and associated risks of managing an inventory of multiple microcontrollers. An example implementation is described in "Case Study: Applicability of CodeGuard Security to Washing Machines". For definitions of the on-chip Boot, Secure and General Segments, see "CodeGuard Security: Definition and Features".

ISSUE: SOFTWARE VENDORS FACE INCREASED RISK OF LOSING IP

In today's global business environment, software vendors increasingly license their IP to unfamiliar parties. Once the IP has been licensed, the buying entity has free access to either source or object code provided by the software vendor. Using the simplest integrated development environments available today, the buying entity can easily translate object code back to source program. While the buyer may never violate the license agreement, there is always the risk of the buyer building their domain expertise by gaining experience using the vendor's IP. In some cases there is a risk that buyers may use their newly gained experience in other projects and need not license the vendor's IP ever again.

SOLUTION: USING CodeGuard Security TO DECREASE RISK OF IP LOSS

CodeGuard Security provides a new method to enable software vendors to decrease the risk associated with loss of IP. Traditionally, software vendors have provided their customers with object files, software protocol stacks or software libraries. These files or libraries are not secure and the underlying source program can be easily exposed using disassembly viewers within an Integrated Development Environment (IDE). Using CodeGuard Security (as shown in Figure 2), software vendors may now program a segment of Flash memory, enable code protection for that segment alone and provide the device to their customer, who can customize the application by adding firmware to a different segment of Flash memory. Software vendors who do not normally provide programmed MCUs or DSCs to their customers can use Microchip or other programming centers or Microchip's Quick-Turn Programming (QTP) process to program devices prior to providing to their customers. Alternately, vendors may use device programmers such as MPLAB® PM3 and MPLAB® ICD 2 to program a segment of memory themselves. Further, software vendors may also provide their customers with any updates to their firmware in the form of encrypted object files. The encrypted object files may be programmed by on-chip bootloaders capable of authentication and decryption. In this case, the advantage provided by CodeGuard Security is that the encrypted hex file can be decrypted within the segment to be re-programmed.

Let us now turn to a simple case that highlights both issues and demonstrates how CodeGuard Security may be used to protect IP.

CASE STUDY: APPLICABILITY OF CODEGUARD SECURITY TO WASHING MACHINES

A washing machine unit comprises a drum unit that includes a Brushless DC motor, a motor controller board with a serial RS-232 interface; and a user-interface board with keypad, LCD, temperature sensors and an RS-232 unit. The user-interface board communicates desired wash load, rinse speed, etc. to the motor controller board via commands over the RS-232 link. Depending on the commands received over the RS-232 link, the motor controller board changes motor speed and torque.

If this application was redesigned for reducing system cost, the MCU in the motor controller board could be integrated with the MCU in the user interface board. However, this is not considered a practical approach because the motor controller board was provided by the entity who manufactures the BLDC motor, whereas the user-interface board is designed in-house by the washing machine manufacturer. Further, the motor manufacturer actually received licensed firmware for the main controller chip of the motor controller board from another software IP vendor. In order to protect his IP, the software IP vendor also insists on code-protecting the MCU on the motor controller board. The BLDC motor manufacturer provides the motor controller MCU to not only the washing machine manufacturer but also to another OEM. In the end, two MCUs are used to fully implement the washing machine product. CodeGuard Security offers a cost-effective, yet secure solution to this problem. Figure 3 illustrates the cost-ineffectiveness issue discussed earlier, as applicable to the washing machine product development. Figure 4 demonstrates how the use of CodeGuard Security can significantly lower system cost, as well as streamline the product development.

FIGURE 3: EXAMPLE: EXISTING WASHING MACHINE DESIGN FLOW

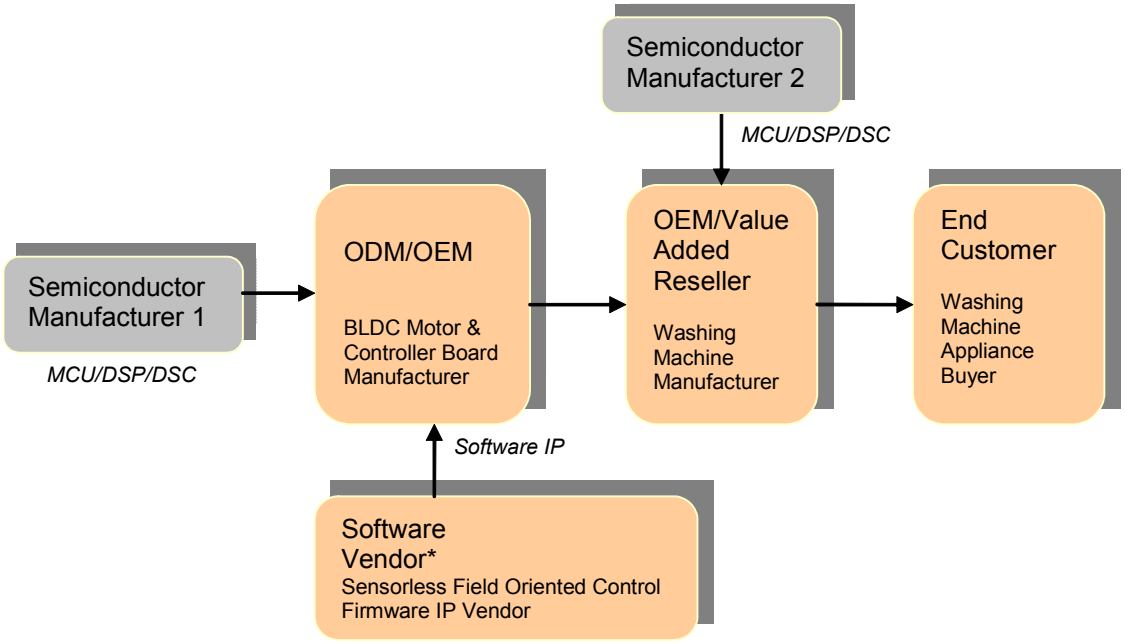
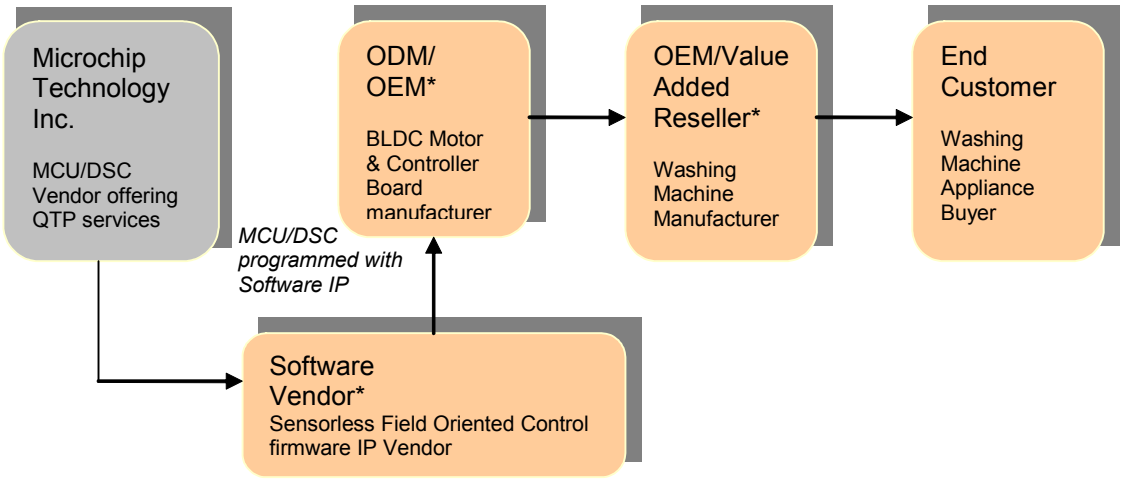


FIGURE 4: WASHING MACHINE REDESIGNED TO INCORPORATE CodeGuard™ Security



Note 1: * Indicates parties who may use code protection features on MCUs, DSPs and DSCs to secure their Intellectual Property (IP).

2: Using CodeGuard™ Security, each party's program may reside in a separate segment of on-chip Flash memory, for instance – OEM bootloader program resides in Boot Segment, software vendor program resides in Secure Segment and VAR program resides in General Segment.

3: This figure shows one of many collaborative design models supported by CodeGuard Security.

Similar examples exist in other applications that involve motors, power conversion, speech, audio, lighting etc. Some examples of the end-applications include automobile air conditioners, HVAC, treadmills, dishwashers, power meters, hands-free phone kits, teleconference equipment, etc.

ISSUE: INSECURE PROGRAM DISTRIBUTION AND FLASH UPDATE

In an increasingly connected world, the need to achieve secure firmware updates or secure data communication is becoming critical. Field-upgradeable Flash microcontrollers are used in many applications in the automotive, consumer and industrial segments. Firmware update of Flash memory in a microcontroller is achieved in many different ways. Whatever the method of update, it is relatively simple to capture both the protocol used to interface with the microcontroller during a Flash update as well as the actual program being updated. For specific examples see “Secure Program Distribution Basics”. A number of MCU and DSC platforms offered by different semiconductor manufacturers are now supported by secure bootloaders that offer the capability to perform secure remote or on-site Flash memory updates. However, these solutions suffer from a few drawbacks:

1. Flash memory updates can be slow and adding a layer of security by attempting to program an encrypted object/hex file makes the process even slower.
2. MCU solutions that offer on-chip hardware encryption are closely tied to specific encryption algorithms or standards and do not support a variety of encryption algorithms.
3. Most MCU solutions do not offer a separate block of Flash memory to store privileged information such as keys associated with encryption and decryption.
4. For the case where software vendors and OEM have collaborated to produce on-chip firmware, no MCU or DSC solutions enable performing an individual secure update of each party’s firmware.

SECURE PROGRAM DISTRIBUTION BASICS

If you are not completely certain about whether your application needs to secure firmware updates of Flash memory, consider the two examples below:

1. A binary/hex file is transmitted to the embedded target using a simple handshake protocol over a serial communication peripheral such as CAN, SPI or RS-232. Logic analyzers probing the serial communication or programming interface pins can provide details on the handshake protocol commands in use as well as the binary pattern contained in the hex file. Thereafter, an unauthorized user can recreate the hex file, modify it using a disassembler, recreate the protocol commands and update the Flash with a different hex file.
2. A binary/hex file is transmitted to the embedded target using a combination of complex protocols and hardware such as TCP/IP and a Modem over a phone line or TCP/IP over an Ethernet link. During the firmware upgrade process, it is fairly simple for a ‘snooping device’ to ‘listen’ to the activity on the communication line and tamper with the embedded application. In the scenario outlined here, the application could be modified without ever having to manually disassemble the hex file or de-solder the embedded target. Steps are provided below:

   A packet analyzer available off-the-shelf can be used to capture CAN messages or TCP/IP packets sent to the embedded target.

   If enough messages or the packets are captured, the protocol governing the program/Flash update is easily deciphered.

   The snooping device can now use the information to send its own messages to the embedded target to tamper with the application. Once again off-the-shelf solutions are available to transmit CAN or TCP/IP messages to the embedded target.

The examples above highlight two security issues:

- Flash memory-based embedded applications are not tamper-resistant
- There is no way to distinguish whether the tampering entity was an authorized or an unauthorized user.

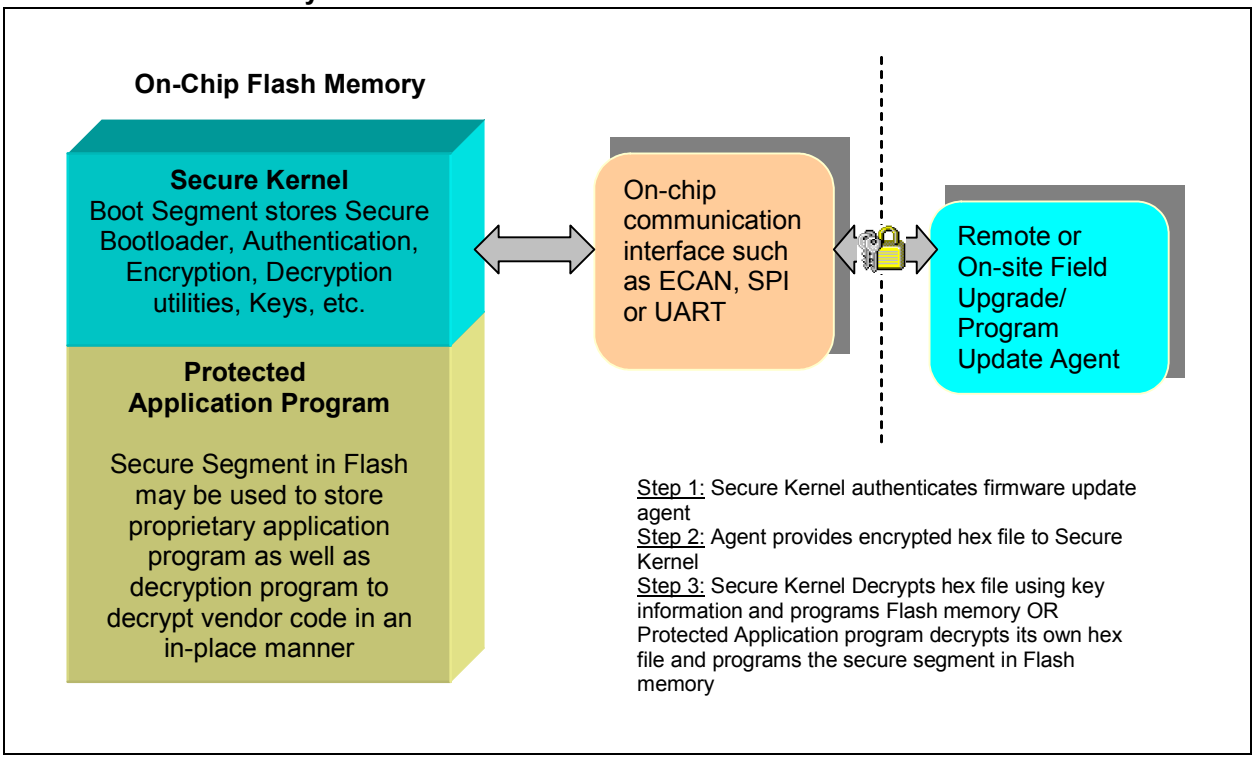
Increasing security against tampering becomes significant to mission-critical systems, such as automotive engine control units or heavy machinery powered by electronically controlled motors. In these applications, mission failures may cause loss of life. The case for adding layers of security in automotive electronics is strong because these systems are already built to support a host of diagnostic utilities and field upgrades.

SOLUTION: USING CodeGuard Security TO SECURE FLASH UPDATE

The four issues with securing program distribution identified in **Section “Issue: Insecure Program Distribution and Flash Update”** are solved using 16-bit MCUs and DSCs featuring CodeGuard Security. Figure 5 shows a potential secure program update model supported by coupling the CodeGuard Security with Microchip’s software encryption libraries. The key items to note are that the CodeGuard Security enables:

1. All decryption and programming firmware can reside within the protected segment
2. Segment Erase options enable faster erase of the on-chip Flash memory, thus speeding up the write/erase time

FIGURE 5: SECURE PROGRAM UPDATE OF ON-CHIP FLASH MEMORY USING CodeGuard™ Security



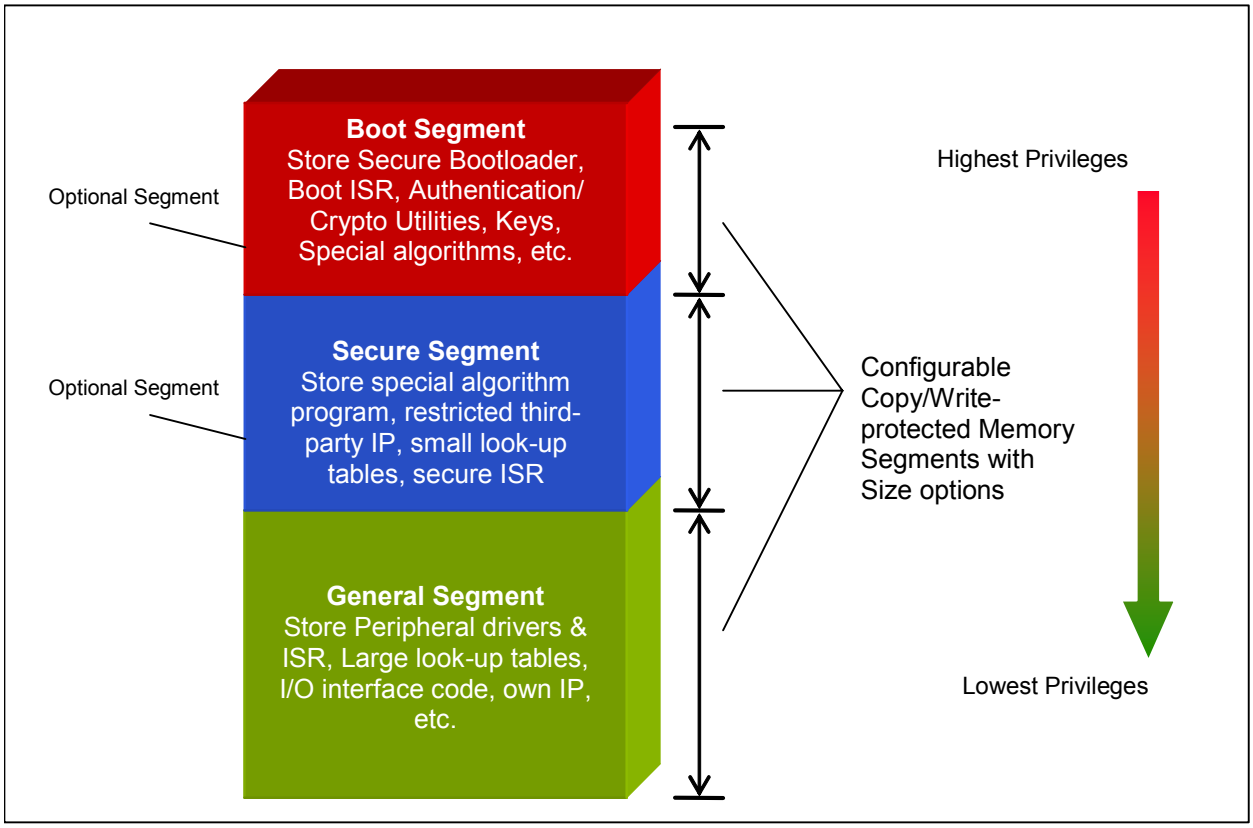
CodeGuard Security: DEFINITION AND FEATURES

The CodeGuard Security provides an advanced code protection scheme to help multiple parties securely share on-chip resources. The features are listed below and discussed later in this section:

- Memory segmentation & access privileges to enable multiple parties to share on-chip resources
- Segment erase/programming options for supporting secure bootloaders/kernels
- Secure interrupt handling
- Secure development and debugging

MEMORY SEGMENTATION FEATURES

FIGURE 6: CodeGuard™ Security – ADVANCED FLASH/RAM/EEPROM MEMORY SEGMENTATION



As shown in Figure 6, the Program Flash memory, RAM and EEPROM in a device featuring CodeGuard Security may be optionally segmented into three protected segments of Flash memory:

- Boot Segment

  The Boot Segment in Flash memory has the highest access privileges of the three segments. The Boot Segment can be configured to be one of many size options. It can be small, allowing a simple yet highly secure bootloader, or large to hold a more sophisticated secure operating system. The Boot Segment can be optionally given the privilege to read from, write to (Flash update), call a routine in or jump to any other segment, code-protected or not. The Boot Segment can also rewrite its own locations, thus allowing the ability to store and update cryptographic keys. On the other hand, if spurious writes are a concern, all Flash writes to the Boot Segment can be completely disabled.

  Access to the Boot Segment from other segments can be limited severely. In the most restricted form (High Security), one can jump to or call a routine in the first few instruction locations of the Boot Segment. In a less restricted setup (Standard Security), subroutine calls and program jumps are allowed from the Secure Segment and the General Segment. Boot Segment can secure portions of on-chip RAM to which access from all other segments are restricted. Boot Segment can also secure portions of on-chip data Flash to which access from all other segments are inhibited.

- Secure Segment

  The Secure Segment is ideal for storing proprietary algorithm routines, such as special motor control software, acoustic noise suppression software, etc. The Secure Segment in Flash memory may be configured for one of many size options. Access to the Secure Segment from the General and Boot Segments can be restricted. Secure Segment can secure portions of on-chip RAM to which access from all other segments is restricted. Program in the Secure Segment of Flash memory can also secure portions of on-chip Data EEPROM to which access from all other segments is restricted. The Boot Segment can be given unrestricted access to the Secure Segment when the Secure Segment is configured for “Standard Security”, but the Secure Segment has identical privileges like the Boot Segment when the segment is configured for “High Security”.

- General Segment

  This segment is ideal for storing the user application program such as peripheral drivers, Interrupt Service Routines, large look-up tables, etc. The General Segment starts immediately following the Secure Segment. Its size is essentially the on-chip Flash memory less the Boot and Secure Segments. If there are no Boot or Secure Segments then the General Segment starts where interrupt vectors end and may be as large as 256KB.

SEGMENT ERASE, PROGRAMMING AND WRITE PROTECTION

The General Segment in Program Flash memory may be individually erased. Erasing the Secure Segment in Flash also causes the Secure Segment in Data EEPROM as well as the General Segment in Flash and Data EEPROM to be erased. Erasing the Boot Segment in Flash also causes all three segments in Flash and Data EEPROM to be erased. Segments in Data EEPROM may be individually erased. Erasing a segment also causes associated Configuration registers for that segment to be erased. During application run-time, the segment erase/programming features facilitate services such as a Secure Bootloader/Kernel that are housed in the Boot Segment. During application development, this feature enables a design engineer to develop program on one segment of the device while another protected segment of the device is already populated with another party's program. Designers also have the option to write-protect each segment of Flash memory to disable any spurious Run-Time Self Programming (RTSP) operations that originate from firmware within the segment.

INTERRUPT HANDLING

In scenarios where two parties share memory resources on a single chip, it is conceivable that program in one protected segment (belonging to one of the two parties) may use peripheral interrupts as a mechanism to interrupt program execution in another protected segment. Even in scenarios where all the program in Flash belongs to the same party, a hacking entity may repeatedly cause external interrupt events to view RAM locations. In all such cases, the hacking entity may be interested in examining temporary registers and RAM locations to establish and even modify the nature of operations being performed by firmware in another protected segment.

CodeGuard™ Security provides special interrupt support to annul such issues. If an interrupt occurs while program executes in one protected segment, the processor vectors to a special interrupt vector within that protected segment. This provides the program an opportunity to save or clear its scratch registers. Once the registers are saved or cleared, the program can examine the pending interrupt request flag and execute a safe branch instruction to the interrupt service routine of the pending interrupt source. By design, the CodeGuard Security provides special interrupt support to protect against data-dumping routines (often termed "Trojan horses"). Further, all 16-bit Microchip MCUs and DSCs support two interrupt vector tables – primary and alternate interrupt vector tables. This feature enables multiple parties to write interrupt service routines for the same peripheral but located in different segments. The ISR to be used can be switched at run time by the application program.

CodeGuard Security: FEATURED PRODUCTS AND AVAILABILITY

CodeGuard Security offers on-chip memory segmentation capabilities in three distinct forms. Devices supporting CodeGuard Security offer one or more of these three forms of memory segmentation. The three forms are described below:

- Basic Form

  In the Basic Form, all on-chip Flash memory is considered one segment (i.e., no segmentation). In this form all of Flash memory is referred to as the General Segment. The application program in the General Segment may be read and write-protected. The Basic Form of segmentation is available on all 16-bit MCU and DSC devices.

- Intermediate Form

  In the Intermediate Form, on-chip Flash memory may be divided into two segments – Boot Segment and General Segment. Programs in each segment may be individually read and write-protected. The Intermediate Form of segmentation is available typically on devices with less Flash memory (48KB or lesser). The Intermediate Form inherently supports the Basic Form through the use of Configuration registers. The Intermediate Form is ideal for low-memory applications in need of secure firmware update features.

- Advanced Form

  In the Advanced Form, on-chip Flash memory, Data EEPROM and Data SRAM may each be optionally divided into three segments – Boot Segment, Secure Segment and General Segment. Each segment may be individually read and write-protected. Further, each segment in Flash may optionally secure a portion of Data EEPROM for its own use. Each segment may also secure or release a portion of SRAM while the application is running. If a segment in Flash memory secures a portion of RAM or EEPROM, other segments do not have access to this RAM or EEPROM. The Advanced Form of segmentation is available typically on devices with Flash memory greater than 48 KB. The Advanced Form inherently supports the Basic and Intermediate Forms by the use of Configuration registers.

CodeGuard Security is available now on all 16-bit products from Microchip. The table below identifies 16-bit Microchip MCUs and DSCs that implement Intermediate and Advanced Forms of CodeGuard Security. It also identifies the largest size that individual memory segments may be configured for. All 16-bit MCUs and DSCs implement the Basic Form of CodeGuard Security, which configures only a single segment in Flash memory.

Device Family	CodeGuard™ Security Implementation Type	Maximum Memory Segment Size (Bytes)		
		Boot Segment	Secure Segment	General Segment
All PIC24F devices	Basic	—	—	All on-chip Flash memory
PIC24H devices with 64KB on-chip Flash memory	Advanced	24K	48K	64K
PIC24H devices with 128KB on-chip Flash memory	Advanced	24K	96K	128K
PIC24H devices with 256KB Flash memory	Advanced	24K	96K	256K
dsPIC30F5011/5013	Advanced	12K	48K	66K
dsPIC30F6010/dsPIC30F6015	Advanced	12K	48K	144K
dsPIC30F6011A/12A	Advanced	12K	48K	132K
dsPIC30F6013A/14A	Advanced	12K	48K	144K
dsPIC30F1010	Intermediate	1.5K	—	6K
dsPIC30F2020/2023	Intermediate	6K	—	12K
All other dsPIC30F devices	Basic	—	—	All on-chip Flash memory
dsPIC33F devices with 64KB on-chip Flash memory	Advanced	24K	48K	64K
dsPIC33F devices with 128KB on-chip Flash memory	Advanced	24K	96K	128K
dsPIC33F devices with 256KB on-chip Flash memory	Advanced	24K	96K	256K

DEVELOPMENT AND DEBUGGING CONSIDERATIONS

DEBUGGING

In the past, numerous hackers have used “processor test modes” or “debug modes” as a back-door to break code protection features. Devices featuring CodeGuard Security have been designed so that program or data in protected segments of Flash, Data EEPROM or RAM are not exposed by disassembly viewers, debug windows, watch windows or test modes.

As previously suggested in this paper, an OEM may procure from a vendor a device with a program resident in the Boot or Secure Segment, with the objective of developing the remainder of the application program in the General Segment. In such cases, in order to aid debugging during the application development phase, the OEM may choose not to enable code protection in the General Segment until the program has been tested and finalized. Thus, CodeGuard Security supports normal debugging of program in unprotected memory segments while rendering invisible the program in the protected memory segments.

DEVELOPMENT TOOLS AND INTEGRATED DEVELOPMENT ENVIRONMENT

Microchip's MPLAB® IDE (v7.41 or later), MPLAB® C30 Compiler Tool suite (v2.03 or later) and MPLAB ICD 2 Debugger support application development on devices featuring CodeGuard Security. MPLAB IDE v7.41 and MPLAB C30 v2.03 are the first releases of the development tools that aid development using the CodeGuard Security. These versions of the development tools support programming of new Configuration registers that protect Boot, Secure and General Segments in Flash memory, Data EEPROM and RAM. Software designers should also note that device-specific linker scripts may need to be further customized to achieve the best results in using CodeGuard Security with these initial versions of the development tools. Future versions of these tools will continue to enhance support for CodeGuard Security.

SECURE FIRMWARE DISTRIBUTION AND FLASH UPDATE SOFTWARE

In order to develop secure kernels secure bootloaders, software design engineers can use Microchip's suite of Symmetric Key (Part Number: SW300050-EVAL) and Asymmetric Key (Part Number: SW300055-EVAL) Embedded Encryption libraries. While the Symmetric Key library supports functions such as Triple DES and 128-bit AES, the Asymmetric Key library supports 1024 or 2048-bit RSA, DSA and Diffie-Hellman. Both libraries feature hash routines such as SHA-1, MD5, and a Deterministic Random Bit Generator. In addition, Microchip also provides Bootloader software freely on the web at http://www.microchip.com.

PROCESS FLOW: FROM SOFTWARE DEVELOPMENT TO PRODUCTION

Since multiple parties may securely share resources on a single chip using CodeGuard Security, some new challenges may arise. These challenges have been identified below and an approach to development has been recommended:

- Which party should program their firmware into the target device first?

  The party which is responsible for programming the segment with the highest privileges (Boot or Secure Segment) should program their firmware into the privileged segment of the device first. In typical cases, this may be the software IP vendor or design house.

- How does one party hand-off the code-protected device to another party?

  When one party programs a higher privileged segment of Flash memory, it can provide the device to the party developing the program for the next highest privileged segment. The device would need to be accompanied by an interface specification that helps the receiving party understand how to call or interface to the code-protected routines. The receiving party also needs the linker script used by the originating party.

- How is programming achieved on the production line when multiple parties own IP that needs to be programmed into the same chip?

  Customers have many options to overcome this challenge. Software IP vendors may use a programming center to program devices with their proprietary algorithm into the Secure Segment (or sometimes Boot Segment). Many programming centers also provide secure bootloaders or kernels that can assist in programming encrypted firmware. Once the IP vendor's firmware is programmed, the programming center can transfer the devices to the OEM's production line or manufacturing center. The OEMs then needs to only program their own firmware into the General Segment (or sometimes Secure Segment) of the device. Once again the OEM may also use the services of a programming center. Microchip provides two kinds of programming services via the microchipDirect Programming Center and the QTP process. For more information on these services, visit our web site at http://www.microchip.com.

SUMMARY

CodeGuard Security available on Microchip Technology Inc.'s 16-bit PIC24 Microcontrollers and dsPIC Digital Signal Controllers adds a unique dimension to the capabilities of the Flash memory based product portfolio. The CodeGuard Security leads a new wave of embedded applications that have come to expect increased security. Coupled with Microchip's software encryption libraries designers can use CodeGuard Security to add valuable features to safeguard their Intellectual Property. For further information on development tools and collateral documentation, please visit our web site at http://www.microchip.com/CodeGuard.

NOTES:

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.

Trademarks

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2002

Microchip received ISO/TS-16949:2002 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona, Gresham, Oregon and Mountain View, California. The Company's quality system processes and procedures are for its PICmicro® 8-bit MCUs, 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://support.microchip.com
Web Address:
www.microchip.com

Atlanta
Alpharetta, GA
Tel: 770-640-0034
Fax: 770-640-0307

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
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Kokomo
Kokomo, IN
Tel: 765-864-8360
Fax: 765-864-8387

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

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Habour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8528-2100
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8676-6200
Fax: 86-28-8676-6599

China - Fuzhou
Tel: 86-591-8750-3506
Fax: 86-591-8750-3521

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

China - Shunde
Tel: 86-757-2839-5507
Fax: 86-757-2839-5571

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7250
Fax: 86-29-8833-7256

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-4182-8400
Fax: 91-80-4182-8422

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

Korea - Gumi
Tel: 82-54-473-4301
Fax: 82-54-473-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Penang
Tel: 60-4-646-8870
Fax: 60-4-646-5086

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-572-9526
Fax: 886-3-572-6459

Taiwan - Kaohsiung
Tel: 886-7-536-4818
Fax: 886-7-536-4803

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-3910
Fax: 43-7242-2244-393

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

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

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

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

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

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

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

07/21/06