Qorivva Architecture Solution: Advanced Security for Body Electronics

Andrew Macleod

Introduction

Unlike powertrain control that has a well defined control loop with microseconds or less to perform the required tasks, the complexity of body electronics is quite different. Sophisticated body electronics applications involve hundreds of tasks running in parallel—essentially hundreds of events that have to be prioritized and executed through multiple and potentially overloaded communication channels.

Responding to driver and passenger requests through (in many cases) switches instead of sensors, the body control module (BCM) activates the air conditioner, heater or fan, raises and lowers windows, moves seats back and forth and locks or unlocks doors, all of which are rather simple functions. In some instances such as temperature control, especially automatic temperature control, the functions are not as simple. Some body electronics aspects and tasks, such as windshield wipers and lighting, are safety-critical functions and have added complexity. Figure 1 shows the architecture of a body electronic control implemented by a single microcontroller (MCU).

Figure 1: Application Block Diagram for Body Control Module (BCM)

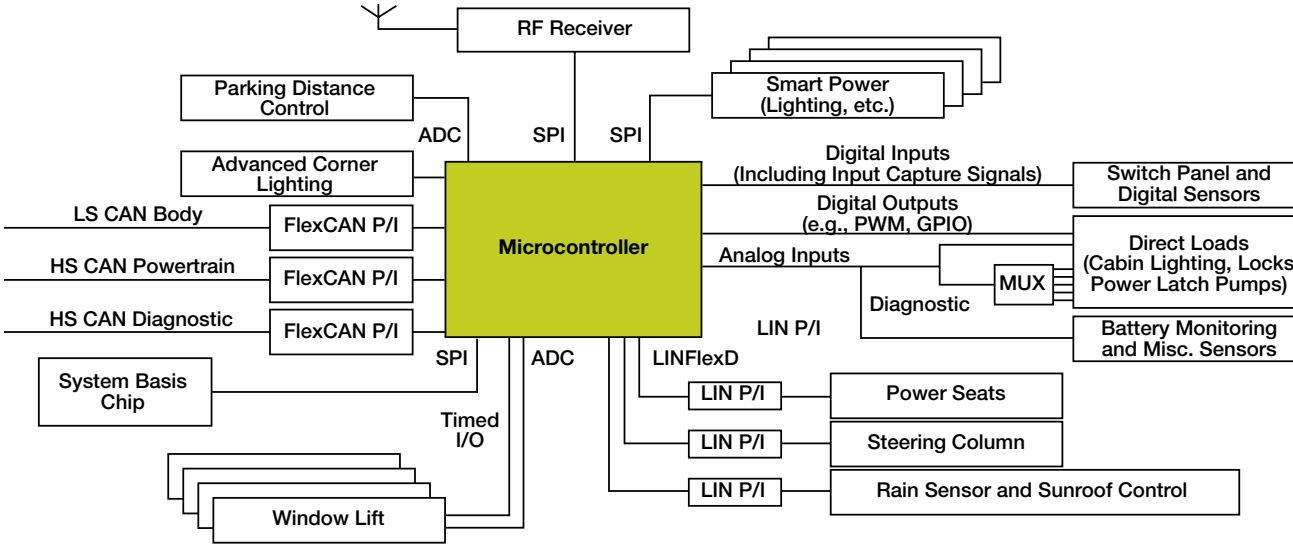
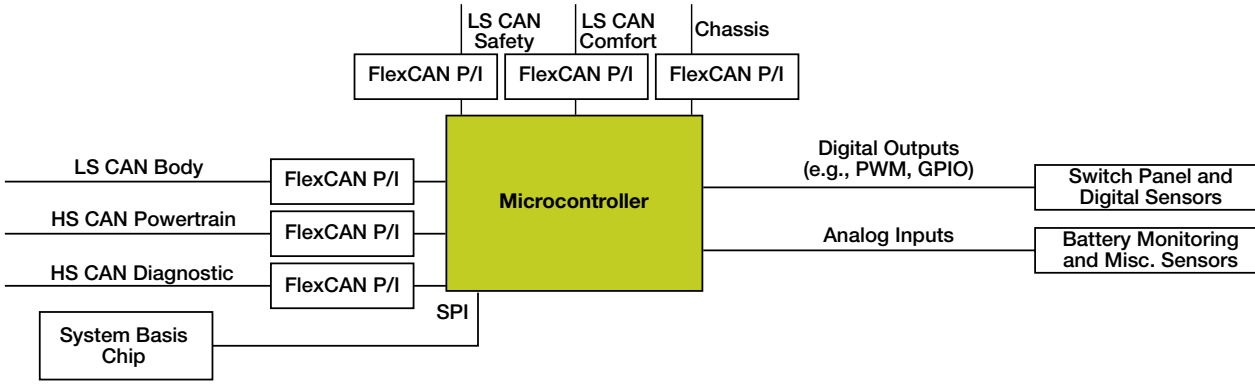


Figure 2: Application Block Diagram for Gateway



Challenges in Implementing Body Electronics Solutions

Although body electronics features are rather simple, the number keeps increasing and they are distributed throughout the vehicle. In fact, many functions are not necessarily in the body controller. Distributed remote functions make body electronics communications intense, especially in gateway applications.

Numerous interrupt-driven tasks require strict software architectures to preserve real-time control. In addition to throughput, bandwidth, memory and the right peripherals, a body electronics MCU must have performance available (sufficient available capacity) to handle a variety of situations.

Reuse of proven, validated software is extensive in body electronics. While simplifying software development, reuse of legacy code requires wrappers around functions—new software to deal with the older software. This layering of software can ultimately create extreme CPU loading.

Finally, body electronics is all about options. As a result, a basic car might only use 1 MB or less of code to support a limited number of options. In a fully featured luxury vehicle, extra modules are added to the control bus requiring more memory in the body control module. However, software in the BCM is the same from low to high end. This requires scalability for the MCUs supporting the range of vehicles. With over 20 years experience in innovating body electronic microcontrollers, Freescale continues to expand the body electronics MCU capability to address the industry's future challenges.

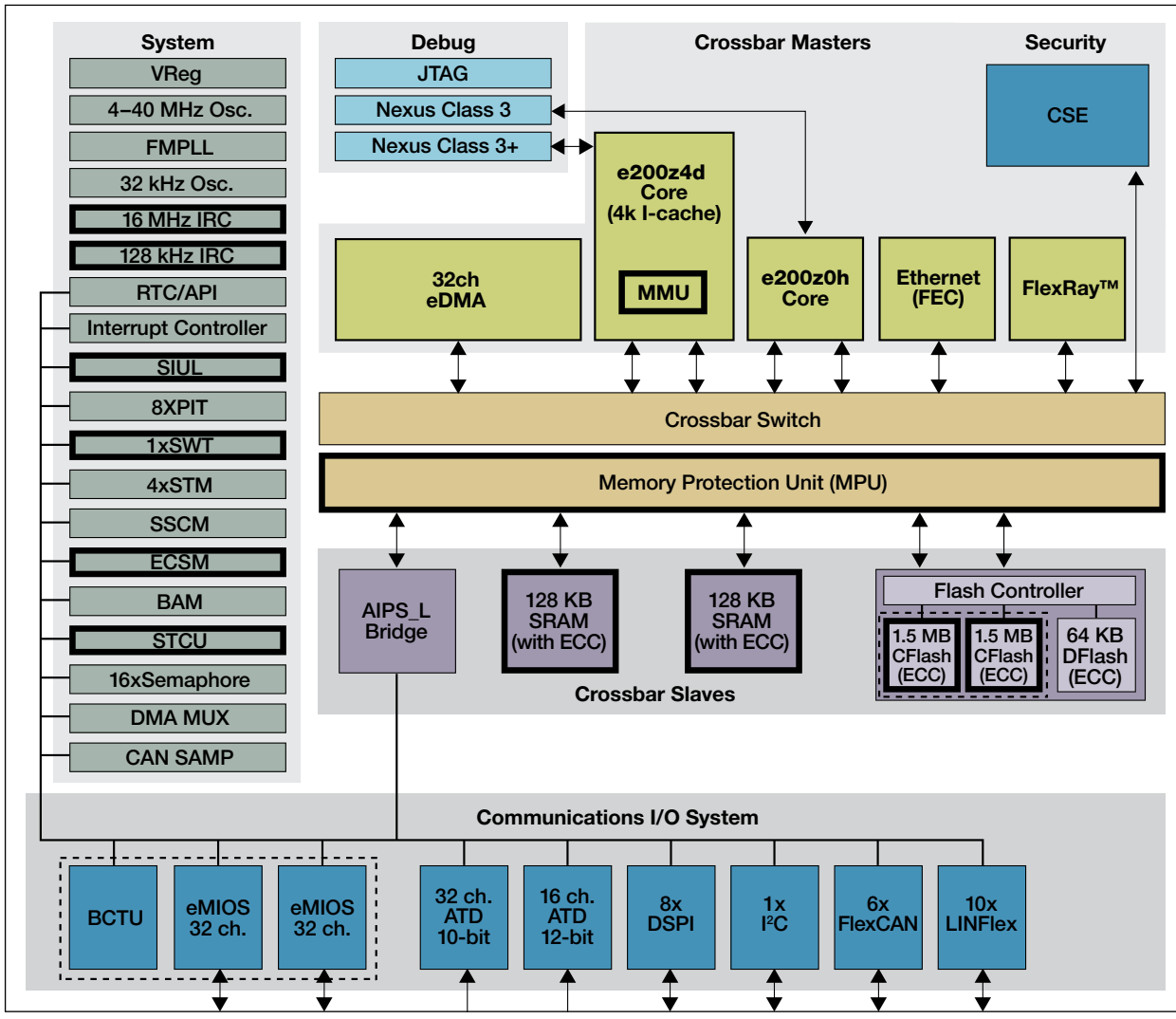
Dealing with Complexity: Qorivva Automotive Microcontrollers

The newest body electronics microcontrollers, MPC564xB/C products, are based on Freescale's Qorivva 32-bit MCUs built on Power Architecture® technology. Initially launched in 1999 for automotive applications, Freescale's 32-bit products are an integral part in many new vehicles. Specifically designed and qualified for automotive applications, the Qorivva architecture encompasses single-core all the way to dual-core and multicore solutions with several connectivity peripherals at the high end.

With the addition of the MPC564xB/C products, Qorivva MCUs provide a 32-bit platform solution, hardware architecture and software framework for body electronics (modules). This allows body electronic module suppliers to avoid completely redesigning a body electronics module for minor function changes between customers. The broad product derivative offering with the MPC564xB/C family can handle different customers' requirements with the same MCU. This provides a simplified system solution for body electronics module suppliers to address with variable hardware and software boundaries.

As a compatible extension to existing products, the newest MPC564xB/C offerings extend the platform to address a wide range of automotive OEM requirements. In addition, MPC564xB/C MCUs bring advanced features like security to automotive applications—one of the first MCUs for the automotive market that incorporate a cryptographic services engine (CSE) that meets the Secure Hardware Encryption (SHE) specification. This specification was developed under the umbrella of the Hersteller Initiative Software (HIS) consortium of European carmakers. As a result of its platform approach, the MPC564xB/C family covers body electronics from top to bottom.

Figure 3: MPC564xB/C Block Diagram



Safety-Relevant Feature

Qorivva Platform Solution

Multicore devices are becoming more common in the automobile because of the benefits they provide for both improved performance and reduced power consumption. In the MPC564xB/C MCUs, the main core can run up to 120 MHz and the smaller core up to 80 MHz to achieve 300 DMIPS. The high-level performance allows the execution of large amounts of code in a CPU-intensive BCM and gateway applications. For reduced power consumption, the main core can be turned off or put in a wait mode, while the smaller core that uses less power runs to check messages and can decide if it needs to wake up the main core to handle a more demanding task. The block diagram in Figure 3 shows the two cores and many advanced features of the newest MPC564xB/C body control MCU.

Distinctive Features of Freescale's Body Electronics Solution

1. Memory options

The newest MPC564xB/C MCUs have from 1.5 MB to 3 MB of flash and up to 256 KB of RAM. The 3 MB of flash is one of the largest amounts in the MPC564xB/C body electronics family and one of the largest in the market.

The large amount of RAM can handle the message buffering required for all the communications peripherals interfacing to the different nodes in body electronics. The 256 KB RAM also supports the requirements of auto-generated software in automotive open system architecture (AUTOSAR). AUTOSAR-based software platforms require more RAM, which this part accommodates. AUTOSAR is increasingly being used in the body gateway applications.

Table 1: MPC564xB/C MCU's Ability to Reduce Power Consumption Using Low-Power Modes

Mode	Condition	Typical	Max
STOP	250ºC	400 µA	1200 µA
STANDBY1 (8 KB RAM retained)	250ºC	25 µA	75 µA
STANDBY2 (64 KB RAM retained)	250ºC	45 µA	135 µA
STANDBY3 (96 KB RAM retained)	250ºC	60 µA	175 µA

2. Low power consumption

The device has several lower power, wait and standby modes to minimize power consumption. Depending on which of the three standby modes is used (see Table 1) current can be reduced from typical values of 60 µA in standby3 down to 45 µA in standby2 to 25 µA in standby1 modes. Internal oscillators support low-power modes and provide fast wake-up.

3. Enhanced communications

As cars incorporate an increasing amount of electronics, the body electronics module's responsibilities increase to handle the additional components and message traffic.

Because of the gateway functionality of the BCM, the MPC564xB/C has enhanced communication capabilities to tackle the extensive communication between CAN, LIN, FlexRay™ and Ethernet buses.

Ethernet is becoming more commonly used for diagnostics for the vehicle and for reprogramming in the factory or in new firmware or software. FlexRay is a communication backbone for safety and chassis networks. CAN and LIN communicate to other body electronics nodes. Table 2 shows the available, cores, memory and Ethernet options for the MPC564xB/C.

Table 2: Six MPC564xB/C MCUs Provide a Variety of Application Options

Features	MPC5644B	MPC5644C	MPC5645B	MPC5645C	MPC5646B	MPC5646C
Cores	e200z4	e200z4+e200z0	e200z4	e200z4+e200z0	e200z4	e200z4+e200z0
Core Frequency	Up to 120 MHz	Up to 120 MHz (z4) Up to 80 MHz (z0)	Up to 120 MHz	Up to 120 MHz (z4) Up to 80 MHz (z0)	Up to 120 MHz	Up to 120 MHz (z4) Up to 80 MHz (z0)
Flash	1.5 MB	1.5 MB	2 MB	2 MB	3 MB	3 MB
RAM	128 KB	192 KB	160 KB	256 KB	192 KB	256 KB
SCI (LINFLEX)	10	10	10	10	10	10
SPI (DSPI)	8	8	8	8	8	8
CAN (FLEXCAN)	6	6	6	6	6	6
FlexRay	Yes	Yes	Yes	Yes	Yes	Yes
Ethernet	No	Yes	No	Yes	No	Yes
Packages	LQFP 176/208	LQFP 176/208 BGA 256	LQFP 176/208	LQFP 176/208 BGA 256	LQFP 176/208	LQFP 176/208 BGA 256

4. Crossbar

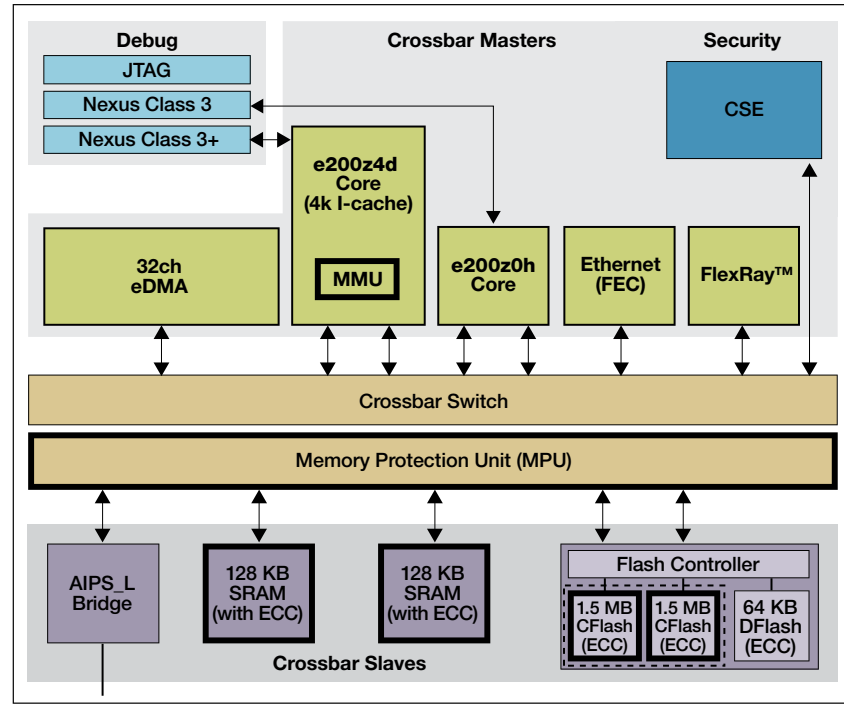
Another important feature of the family is the crossbar, an architectural concept that provides additional performance and scalability. As shown in Figure 4, the crossbar consists of masters, slaves, a crossbar switch and a memory protection unit. The crossbar switch allows parallel access between masters and slaves and another means to maximize performance.

With the crossbar, any master can communicate with any slave, while a different master is simultaneously talking to a different slave. For example, the core can access data from flash memory while the DMA communicates over the communications bridge to a DSPI module to obtain a message transmitted from another module. Meanwhile, the Ethernet module stores incoming messages in a separate RAM block as the DMA is being used to download new code.

This parallel operation provides a higher performance level because the MCU does not have to wait for the completion of one data transfer before starting another. The crossbar performs the same functions on a low-end or high-end MCU—only the number of data paths changes. This function can also provide memory mapping (flash and RAM) for additional performance in multicore scenarios optimizing where data and code is stored to maximize the use of the crossbar.

As features are added to the product family in the architecture, such as an Ethernet port, the crossbar creates a data path to the RAM so the new feature has a minimal performance penalty. The crossbar handles the added requirements without creating excessive overhead on the system.

Figure 4: Crossbar Allows Parallel Access to On-Chip Resources



Safety-Relevant Feature

5. Safety-relevant functionality

There are four specific safety areas in body control: front lighting, windshield wipers, rear brake lights and the steering column lock. Qorivva designers incorporated several features to improve the system's dependability and robustness. (See identified safety-relevant areas in Figure 3). Without the safety-relevant features of the MPC564xB/C, redundancy must be added to the system to ensure proper operation of these functions.

6. AUTOSAR ready/compliant

MPC564xB/C MCUs are ready to support AUTOSAR 4.0. AUTOSAR is open and standardized automotive software architecture, jointly developed by automobile manufacturers, suppliers and tool developers. It specifies the low-level drivers and operating systems that allow automotive microcontrollers to share resources across most applications.

AUTOSAR has progressed from a 1.0 to 3.x version today, however the 4.0 version is imminent. It exists as a draft specification today and its release is expected in the second half of 2011. AUTOSAR 4.0 will be the first version to include multicore support. With AUTOSAR specifications in place for this support, multicore architectures can be easily designed into vehicles. As a member of AUTOSAR and an integral part of the development of AUTOSAR 4.0 with the MPC564xB/C, Freescale is prepared to be one of the first implementers of a multicore architecture that is AUTOSAR 4.0 ready.

7. Security

Modern vehicles have an increasing need for security. As shown in Table 3, security applications include immobilizers to prevent car theft, component protection for modules, and protection against data theft such as tampering with the mileage on the car. Security can also prevent tuning or modifying anything that would violate the warranty, as well as protecting personal information, such as a phone book or any financial information for transactions that occur in the vehicle.

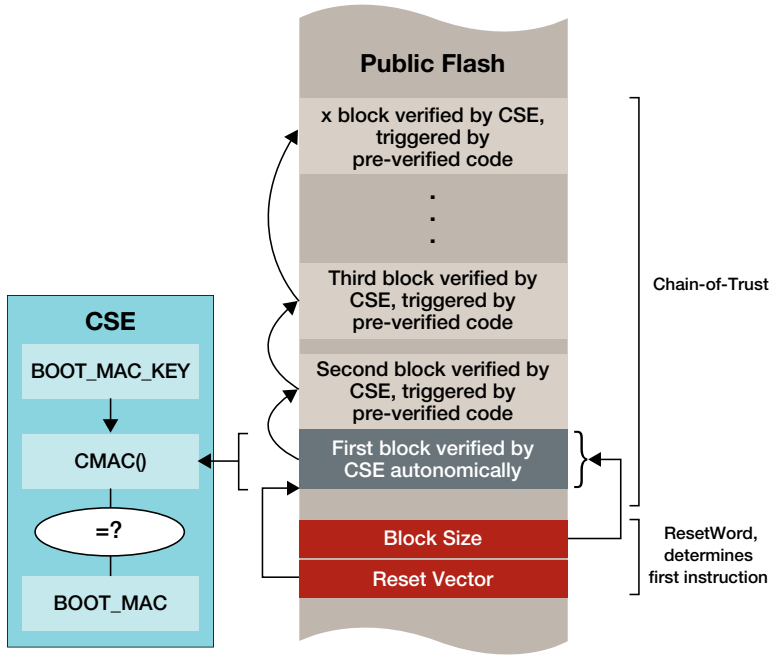
In the future, the need for a high level of security will expand far beyond today's applications. Cars are expected to hold even more information as they become smart cards on wheels to simplify financial transactions at gas pumps, charging stations, parking lots, toll booths, drive-thru establishments and more. The vehicle will act as a smart card and pay your fee/fare—sometimes automatically.

There are many ways that security is implemented today, but the MPC564xB/C is the first product to meet the SHE specification. The SHE spec moves the control of the security keys from software into the hardware domain and protects the keys from software attacks.

Hardware-based security is more robust than software-only security. The MPC564xB/C has additional features that improve on that security.

The cryptographic services engine (CSE) designed by Freescale implements the SHE specification. Non-volatile as well as RAM memory protected within the core contains data that is only accessible via the CSE module. The CSE provides a hardware location for the security keys. In addition to the keys, the module has cryptographic algorithms that it can accelerate including the National Institute of Standards and Technology (NIST) AES-128 standard.

Figure 5: CSE and Secure-Boot Process for Vehicle Security Applications



The secure boot is the basis for establishing the root for trust for all of the use cases in Table 3. Without secure boot, the others will not work or have compromised security. As shown in Figure 5, when the module first starts up, the CSE module checks a small section of the flash module and verifies that all the content in that section is correct.

The CSE module then checks each remaining section until it has verified the entire flash array to ensure that it has not been tampered with since the last start-up. The CSE offers cryptographic services only if the flash integrity was proven.

After it verifies that it is dealing with a secure environment and ensures that the device itself has not been compromised/hacked in the public flash area, the CSE transmits encrypted data to and from the public flash. This is one of the unique capabilities of MPC564xB/C. Secure-boot helps to verify the system integrity via the cipher-based MAC algorithm.

Table 3: Security Use Cases/ Applications in Automotive Body Electronics

Immobilizers
Component protection
Flash updates
Protecting data sets (e.g. mileage)/ prevent chip tuning
Protecting personal information (last destination, phone book etc.)
Feature management (e.g. navigation map) and digital rights management (DRM)
Secure communication
Secure communication
Protecting software and IP
Secure boot

Conclusion

Similar to other Freescale automotive electronics firsts, the Qorivva architecture has its own firsts for the body electronics market. Qorivva family firsts include: The first body control MCU with 3 MB of flash memory, the first with cryptography and the first multicore AUTOSAR 4.0-ready device.

The award-winning family (recognized by Design & Electronik's embedded Award 2011 in the hardware category) also has the validation of customers with multiple design wins that confirm the value of the architecture.

Designed for body electronics, the Qorivva architecture and MPC564xB/C MCUs have the ability to handle a wide range of applications. The MCU platform solution provides the foundation for tier one body control module platform solutions to easily address automotive requirements from low-end to high-end vehicles with the security that carmakers demand—now and in the future.

How to Reach Us:

Home Page:
freescale.com

Power Architecture Portfolio Information:
freescale.com/power

e-mail:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
1-800-521-6274
480-768-2130
support@freescale.com

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014
+81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447
303-675-2140
Fax: 303-675 2150
LDCForFreescaleSemiconductor@hibbertgroup.com

freescale™

For more information, visit freescale.com/power

Document Number: PWRARBYNDBITSQAS REV 0

BUILT ON Power™