Transitioning the Plug-In Industry from Legacy to UEFI: Real World Cases and Call to Action

Steve Jones
Chief Scientist, VP Core Systems, Phoenix Technologies Ltd.

Michael Krau
Senior Technical Marketing Engineer, Intel Corporation

EFIS005

Sponsors of Tomorrow.™ intel

Agenda

- Plug-Ins! Past, Present, and Future
- UEFI is Making BIOS Plug-Ins Possible!
- Real World Examples
- Taking Plug-Ins to the Next Level
- Call to Action

Plug-Ins: Added Value for PCs

Plug-Ins are added value for PCs installed by either:

- The OEM
- The End User

What plug-ins do we use today?

For MP3 players, it's earphones, power supplies, etc.

For PDAs/smart phones, it's app store software

For PCs, plug-ins extend functionality too

Plug-Ins: Added Value for PCs

- OEM Plug-Ins:
  - Likely to exist in source code form
  - Require technical integration into the BIOS in some way (source, adaptation, etc.)
  - Integrated as part of system test
- User Plug-Ins:
  - Need seamless binary installation
  - Lots of issues (security, storage, configuration, compatibility, etc.)
  - Must just work without any “system test” on the user’s part

Plug-Ins: Added Value for PCs

- In the early days, plug-ins made hardware operational– ROM BIOS extensions (OpROMs)
- Today's add value is less about new hardware options, and more about other things:
  - **Virus/Malware Protection**
  - **Enterprise Management**
  - **OS Installation**
  - **Geo-Fencing**
  - **Instant-On environments**
  - **Diagnostics**

Plug-Ins Past and Present

Today's computing is trending towards enclosed systems with limited hardware expansion

1981-1989

Expansion via hardware plug-ins (i.e. LAN, Modem, Graphics)

1990-1999

USB PCI SIG

Expansion via standards (USB, PCI)
Early Notebooks with limited expansion
Connectivity: Network, Internet

2000-2009

Accelerated Transition to Mobility (Notebooks, Netbooks, PDAs, etc.)
Limited Expansion: Closed Systems

Plug-Ins: Near Future

What forces are driving plug-ins now?

- 2010 : UEFI Notebooks: SW Door Opens
  - 2008-2009: Steady growth in UEFI adoption
  - 2010*: Broad adoption of UEFI: ~>50% notebooks shipped
- 2012** : Form Factor Mobile UEFI Adoption
  - i.e. PDAs, Mobile Phones, MP3 players, etc.

* Source, UEFI Forum
** Source, Phoenix Technologies

Plug-Ins: Longer-Term Future

What forces are driving plug-ins later?

- 2015*: The Cloud: Unlimited storage and services
- 2015*: The Grid: Unlimited computing power
- 2020*: Shift from “press this to cause the device to do that” to peer interaction with the device

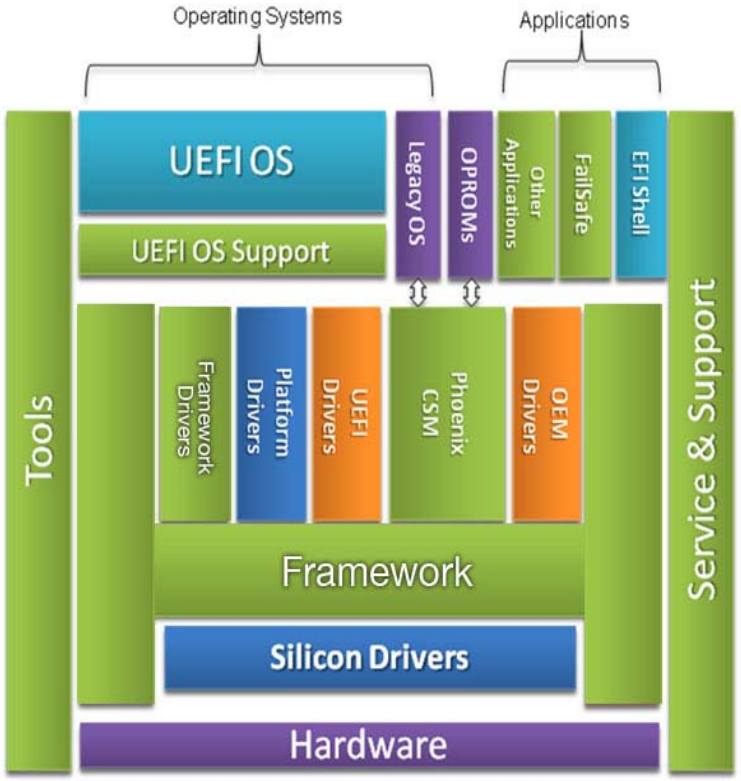
* Source, Phoenix Technologies

Agenda

- Plug-Ins! Past, Present, and Future
- UEFI is Making BIOS Plug-Ins Possible!
- Real World Examples
- Taking Plug-Ins to the Next Level
- Call to Action

UEFI is Making Plug-Ins Possible!

- Focus on Mobile Devices
- All new systems shipping with some form of UEFI
- Phoenix creating UEFI solutions for all new silicon solutions
- Green H: Formal packaging of executable entities, run-order, flow control
  - Does away with hooking and patching



Green H/UEFI Transforms Plug-Ins

	Legacy	UEFI
Memory Allocation	☹ BDA Editing ☹ INT 15h	✓ Allocate Pages ✓ Allocate Memory
I/O to Screen	☹ INT 10h/INT 16h ☹ Painting video memory	✓ ConIn/ConOut handles
Hotkeys	☹ Hook INT 09h, INT 08h, INT 1ch	✓ Hotkey protocols
Security	☹ None	✓ Well Defined Protocols
Configuration	☹ ^S to enter special setup program in ROM	✓ Human Interface (HII) Protocols
Packaging	☹ ROM extension on PC card	✓ UEFI DXE Driver ✓ UEFI Application

UEFI offers Standard services & Interfaces vs. ad-hoc legacy implementation

Agenda

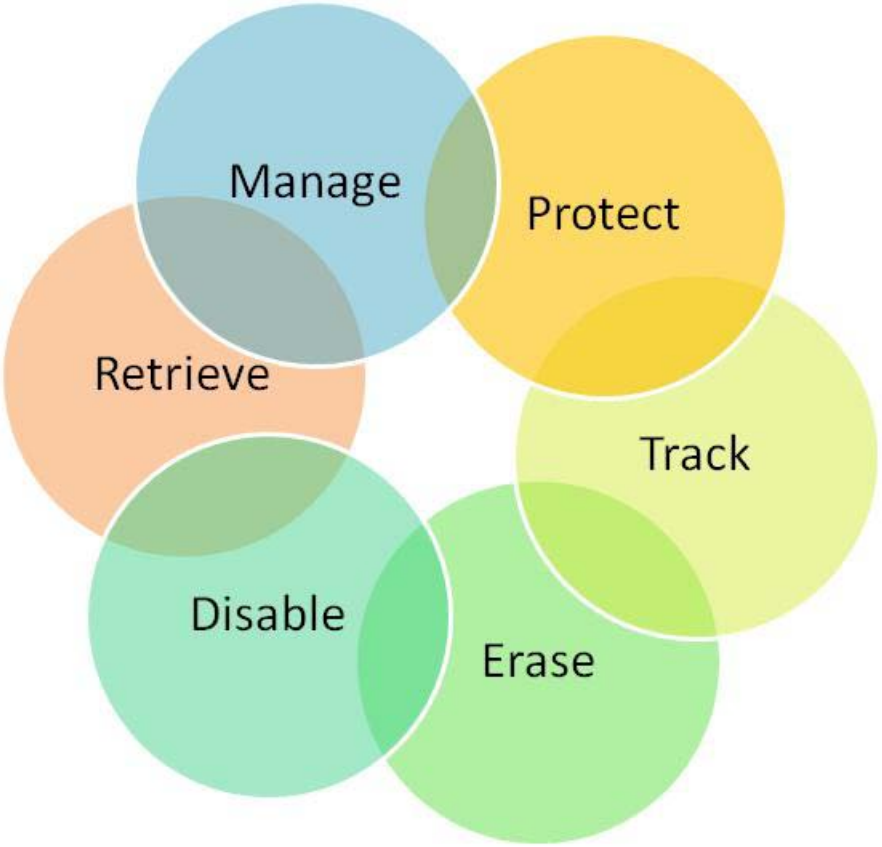
- Past, Present, and Future of Plug-Ins
- UEFI is Making BIOS Plug-Ins Possible!
- Real World Examples
- Taking Plug-Ins to the Next Level
- Call to Action

Real World Example-Phoenix FailSafe™

- Deployed on legacy BIOS and UEFI systems
- Deployed on Phoenix SecureCore™ /Legacy
- Deployed on Phoenix SecureCore Tiano™
- Deployed on other IBV offerings!

Case Study #1: FailSafe™ – What is it?

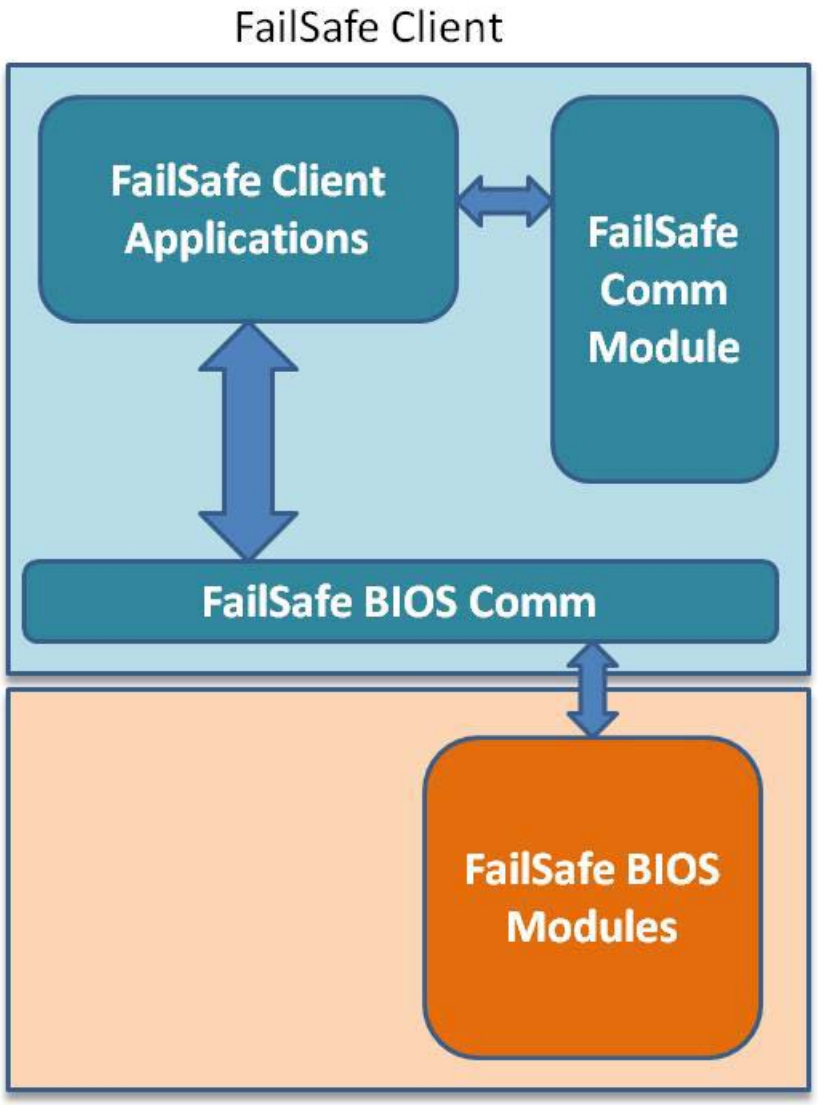
A SaaS offering from Phoenix Technologies that provides the ability to protect, track and remotely manage lost or stolen notebook or netbook



FailSafe
Secure your laptop

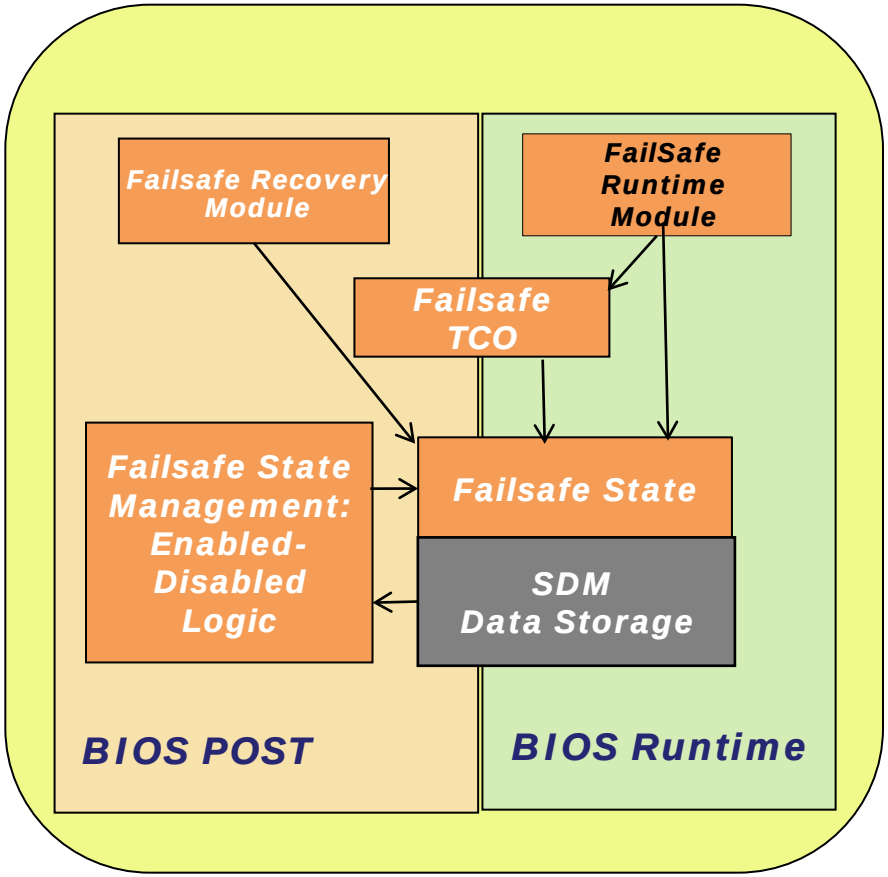
Case Study #1: FailSafe™ – What is it?

- Lock laptop at the BIOS level
- BIOS stores critical information
- Cryptography modules in BIOS responsible for authenticating callers
- Uses UEFI SMM architecture to perform all runtime operations



FailSafe Legacy Implementation

- Created as a Phoenix SecureCore feature
- Tightly coupled with SecureCore features
  - Secure BIOS-to-OS communication (CryptOSD)
  - Encrypted data storage (SDM)
  - Cryptographic features (StrongROM)
  - Additional features
    - Hard-disk password support
    - User password collection routines



FailSafe™ – Legacy Porting Challenges

- Option ROM concept dismissed
  - Cannot use platform setup screen
  - No conflict-free mechanism for CMOS access
  - Prone to malware attacks

- Tight integration with 3rd party BIOS
  - Little knowledge of the architecture
  - Need to integrate key SecureCore features/services
  - OS compatibility with SecureCore™
  - SDK for ease of implementation – difficult to generalize

FailSafe™ SDK (Legacy)– Binaries

- SDK created as a proprietary binary solution
- Additional effort required by 3rd party BIOS teams:
  - Six binary modules in flash
  - Memory allocation
    - i.e. E000/F000 and SMM
  - Placement of SDK binaries in specific regions
  - Population of binary headers with environment information

FailSafe™ SDK (Legacy)– Challenges

- SDK solution had large code size driven by:
  - Time to market urgency
  - Lack of familiarity with the code
  - Lack of common services
- Unexpected environment differences:
  - SDK assumed SMM code address at TSEG vs. a flat address
- Conflicting behaviors:
  - FailSafe hard-disk password implementation compatibility with 3rd party BIOS solution

Failsafe™ – UEFI Implementation

- EDK framework as a starting base
- Greater modularity and portability through UEFI services and protocols
  - Boot Services and Runtime Services
    - **Readytoboot**
    - **LegacyBoot,**
    - **Exitbootservices**
  - User Interface
    - **Conin()**
    - **Conout()**
  - Wide array of UEFI protocols
    - **EFI_CPU_IO_PROTOCOL**
    - **EFI_SMM_CPU_PROTOCOL**
    - **EFI_ACPI_SUPPORT_PROTOCOL**
    - **EFI_LEGACY_BIOS_PROTOCOL**
    - **Etc.**

UEFI significantly improves portability across multiple code bases

Failsafe: UEFI Challenges

- Not all BIOS codebases are compliant with the latest spec
  - Some protocols not yet adopted by everyone
    - EFI_SMM_COMMUNICATION_PROTOCOL
    - EFI_SMM_CPU_PROTOCOL
- Build environments are different, require additional integration effort
  - SDK is released for a EDK style build environment
    - Adding new binaries to build requires ".inf" and ".dxs" files
  - Lack of standardization on global settings/environment variables

➢ *Need a standard build environment or means for binary inclusion*
➢ *Compliance checking and plugfests are a must*

Agenda

- Let's Talk Plug-Ins!
- Past, Present, and Future of Plug-Ins
- UEFI is Making BIOS Plug-Ins Possible!
- Real World Examples
- Taking Plug-Ins to the Next Level
- Call to Action

Taking Plug-Ins to the Next Level

- Preparation for transition from OEM “Push” to End User “Pull” in the market

- Solve User-Level problems, not OEM problems

Taking Plug-Ins to the Next Level

- Make Mobile Systems Plug-In Friendly (OEM/ODMs)
  - Need to create concept vehicles

- Make Tools that are Plug-In Friendly (IBVs)
  - Create SDKs for ODMs and OEMs

  Also
  - Create SDKs for Plug-In Makers
  - Development environment that abstracts the complexities of BIOS from the Plug-In makers

i.e., You don't need Windows 7* source code to create a Windows application.

Taking Plug-Ins to the Next Level

- IBVs to collaborate with UEFI forum and define a path to move to binary distribution (i.e. app store level)

- All IBVs will have their own ideas

- Phoenix is working on:
  - **Installation** – Installer
  - **Discovery** – Defining firmware volume assignments for plug-In storage
  - **Compatibility** – UI form and function
  - **Storage** – Read/Write firmware volume assignments and QoS for data storage
  - **Isolation** – Adding protection around apps for security and reliability
  - **Performance** – One second POST
  - **Power Management** – Best practices for maximizing battery life
  - **Configuration** – Best practices to simplify user experience

Agenda

- Let's Talk Plug-Ins!
- Past, Present, and Future of Plug-Ins
- UEFI is Making BIOS Plug-Ins Possible!
- Real World Examples
- Taking Plug-Ins to the Next Level
- Call to Action

Call To Action

- Plug-Ins are going to take off, as the role of the BIOS/Pre-Boot is standardized and stabilized
- Importance of Plug-Ins will increase
  - Allows for differentiation and expandability in otherwise closed systems
- IBVs, ODMs, OEMs, and SVs will pave the way for plug-In manufacturers to add value:
  - First at the source code level as they sell to OEMs
  - Finally at the binary level as end users install their own plug-ins

Active participation in the UEFI Forum is key to the success of plug-ins

Additional resources on UEFI:

- Visit UEFI Booth #136
- More web based info:
  - Specifications and Implementation sites: www.tianocore.org, www.uefi.org, www.intel.com/technology/efi
- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress

Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessions

Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events

Q&A

Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.
- Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
- Copyright © 2009 Intel Corporation.

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the third quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel's actual results, and variances from Intel's current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation's expectations. Ongoing uncertainty in global economic conditions pose a risk to the overall economy as consumers and businesses may defer purchases in response to tighter credit and negative financial news, which could negatively affect product demand and other related matters. Consequently, demand could be different from Intel's expectations due to factors including changes in business and economic conditions, including conditions in the credit market that could affect consumer confidence; customer acceptance of Intel's and competitors' products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Additionally, Intel is in the process of transitioning to its next generation of products on 32nm process technology, and there could be execution issues associated with these changes, including product defects and errata along with lower than anticipated manufacturing yields. Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel's response to such actions; and Intel's ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; capacity utilization; start-up costs, including costs associated with the new 32nm process technology; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; product mix and pricing; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; and the timing and execution of the manufacturing ramp and associated costs. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The current financial stress affecting the banking system and financial markets and the going concern threats to investment banks and other financial institutions have resulted in a tightening in the credit markets, a reduced level of liquidity in many financial markets, and heightened volatility in fixed income, credit and equity markets. There could be a number of follow-on effects from the credit crisis on Intel's business, including insolvency of key suppliers resulting in product delays; inability of customers to obtain credit to finance purchases of our products and/or customer insolvencies; counterparty failures negatively impacting our treasury operations; increased expense or inability to obtain short-term financing of Intel's operations from the issuance of commercial paper; and increased impairments from the inability of investee companies to obtain financing. The majority of our non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management's plans with respect to our investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. A detailed discussion of these and other risk factors that could affect Intel's results is included in Intel's SEC filings, including the report on Form 10-Q for the quarter ended June 27, 2009.