Panel: Using Unified Extensible Firmware Interface (UEFI) as the Foundation for Innovation

Mark Doran - Senior Principal Engineer, Intel
Sean Brogan - Senior Software Engineer, IBM
Anand Joshi - Senior Software Engineer, Dell
Dong Wei - Distinguished Technologist, HP
Peter Brundrett - Principal Program Manager, Microsoft

EFIP001
Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products
Agenda

• UEFI Technical Specifications updates

• Using UEFI as an enabling foundation for platform innovation

• Industry leaders discussing how UEFI is helping them innovate and differentiate their products
Standard Firmware Interfaces

- **UEFI**: Unified Extensible Firmware Interface
  - a new model for the interface between the OS and platform firmware

- **PI**: Platform Initialization
  - Standardization: key to interoperability across implementations
  - Modular components like silicon drivers (e.g. PCI) and value-add drivers (security)
  - Preferred way to build UEFI

**UEFI is Architected for Dynamic Modularity**
Latest UEFI Specifications

- Platform Initialization (PI) 1.2 Spec
- Packaging 1.0 Spec
- UEFI 2.3 Spec
- Self Certification Tests (SCT) for UEFI 2.1 Spec
- Shell 2.0 Spec

Advancements in firmware technologies continue to evolve. Join the UEFI forum www.UEFI.org
UEFI Specification Timeline

UEFI 2.0
UEFI 2.1
UEFI 2.2
UEFI 2.3
PI 1.0
PI 1.1
PI 1.2
Shell 2.0
Packaging 1.0
2006 2007 2008 2009 2010
SCT UEFI 2.0
SCT UEFI 2.1
EDK 1.01: UEFI 2.0
EDK 1.04: UEFI 2.1
EDK 1.05: UEFI 2.1+
PI 1.0
PI 1.0
Open Source
Upcoming
EDK II: UEFI 2.3+
EDK II: UEFI 2.1+
PI 1.0

All products, dates, and programs are based on current expectations and subject to change without notice.
Agenda

• UEFI Technical Specifications updates
• Using UEFI as an enabling foundation for platform innovation
• Industry leaders discussing how UEFI is helping them innovate and differentiate their products
Utilize UEFI Full Potential

Limited Benefits:
- OEMs/ODMs internal Development Optimization & Code Modularity

Full Benefits:
- UEFI Innovation
- Performance
- Extensibility
- Advanced Usability

Build UEFI Class 2/3 UEFI Systems!

1 Compatibility Support Module – Legacy BIOS interface on top of UEFI
**UEFI Enabling Platform Innovation**  
*Modern Firmware for Modern IT*

<table>
<thead>
<tr>
<th>Easier to configure and deploy</th>
<th>Makes Computers more manageable</th>
<th>Network Scalable and Secure Firmware</th>
<th>Breaks through BIOS barriers</th>
</tr>
</thead>
</table>
| • Richer configuration (allows for more adapters)  
• Graphic User Interface in Pre-boot environment  
• Remote upgrade capability of specific firmware components  
• Solves out-of-the-box configuration & provisioning issues | • Creates a common infrastructure for managing all machines  
• Enable secure automated management – lower risks of “Rogue” servers or clients on the network | • Enhanced networking APIs in the pre-boot network stack  
• Richer network authentication (log-on)  
• UEFI Certificate Authority for interoperable trust | • Free from architectural limitation - scales technology across all platforms (Server, Desktop, Mobile, and Handheld)  
• Access to disk range beyond 2TB – utilization of resources  
• Option Rom Decongestion |

*IDF2009*

*INTEL DEVELOPER FORUM*
Agenda

• UEFI Technical Specifications updates
• Using UEFI as an enabling foundation for platform innovation
• Industry leaders discussing how UEFI is helping them innovate and differentiate their products
UEFI Adoption

UEFI Technology is the primary firmware reference of choice for Intel® Xeon® 5500 Processor based Platforms

Growing UEFI Community
Major MNCs shipping UEFI

Source: UEFI Forum Media Advisory For Spring’08
IBM Innovations using:
Unified Extensible Firmware Interface (UEFI) &
Platform Initialization (PI)

Sean Brogan - Senior Software Engineer,
IBM Systems and Technology Group
System X Servers

- Comprehensive transition of the System x portfolio to UEFI based firmware
- UEFI 2.1 PI 1.0 specification compliant
- Improved management and configuration capabilities
- Advanced “Touchless” Compatibility Support Module (CSM)
- Trusted Platform features: TPM enablement, TCG and Core Root for Measurement support

Blade
- HS22

Rack-mount
- x3650 M2
- x3550 M2
- X3250 M3

Tower
- x3500 M2
- x3400 M2
- x3200 M3

Large-scale
- dx360 M2*

* System does not support Trusted Platform features
Advancing the platform

- Complete UEFI 2.1 / PI 1.0 firmware implementation (Power on to boot selection)

- Strong/Modular framework
  - Global Development (4+ time zones)
  - Interoperability with Internal teams, partners, and vendors
  - Allowing feature based development
  - Common code base

- Seamlessly support legacy environment
  - IBM Surepath CSM (Legacy x86 BIOS support for legacy OS support)
  - Touchless CSM invocation - auto detection of boot option (UEFI/legacy)
  - UEFI Class 2 – supporting both UEFI boot and legacy boot Operating Systems

- Standardized Pre-boot Security
  - TPM\(^1\) hardware enablement
  - TCG\(^2\) and Core Root of Trust for Measurement support (CRTM)
  - Secure Update methods
  - Attend IDF Session EFIS001 for more details
  - IBM/Intel collaborative Whitepaper “Trusted Platforms: UEFI, PI and TCG-based firmware”
Future areas of investigation

- IBM Enterprise system support
- EDKII development environment
- Specification Evolution (UEFI 2.2+ and PI 1.1+)
  - IPV6
  - UEFI certificate authority with driver and module signing
  - Out of Band management capabilities

**UEFI provides a great foundation for innovation!**
UEFI AND DELL

Anand Joshi
Sr. Software Development Engineer, Dell
- UEFI defines a standard software “bus”
- Plug-in modules from different suppliers can co-exist
  - Silicon suppliers
  - Open Source
  - Dell IP
  - 3rd party
- Creates an attractive, standardized market for 3rd party firmware component suppliers
- Enables code development/collaboration with Dell’s partner’s
UEFI On Dell Servers

Dell PowerEdge servers based on Intel Series 5500 processor feature UEFI 2.1

Modula:
- M610
- M710

Rack
- R410
- R610
- R710

Tower
- T310
- T410
- T610
- T710
INNOVATION

• Enhanced pre-boot space
  – Improved Graphical User Interface
  – Network support
  – USB hot plug

• Better manageability
  – Common configuration Interface through HII
  – Intelligent, Efficient Platform Updates
  – Flexible OS deployment
HP UEFI Status

Dong Wei
Distinguished Technologist
UEFI Board Member (HP)
HP UEFI Support Status

- **HP Printers/Scanners**
  - Color Multifunction Printer (shipped)
  - ScanJet Enterprise 7000n/nx Document Capture Workstation (to be shipped)
- **HP Notebooks and Tablet PCs**
  - HP innovating based on the UEFI technology: e.g., Diag
  - Commercial systems support UEFI boot
- **HP Desktops and Workstations**
  - Adopt a common UEFI codebase
  - Collaborate with Commercial Notebooks on HP features that provide enhanced manageability, security and ease of use
- **HP Integrity Business Critical Servers**
  - HP-UX, Windows, Linux, OpenVMS, HP Integrity Virtual Machine operating environments use UEFI
- **HP StorageWorks**
  - Using UEFI to deliver next generation storage arrays
- **UEFI/PI framework has enabled code sharing opportunities among business entities and with partners/vendors.**
Innovations

• Enhanced Diagnostics
  − DIMM fault isolation
  − Hard drive simultaneous test
  − Concurrent memory, hard drive and batteries test
  − Improve test coverage, optimize test cycles

• Cost Savings
  • Shift resources towards differentiation and innovation
  • Reuse common modules across product segments
  • Converged EDK strategy would enable faster and wider industry adoption, removes unnecessary waste in resources porting across codebases

• Areas of Future Explorations
  − Better user experience via HII
  − More secure platform via image signing
  − IPv6 network
Microsoft on
UEFI and Platform Innovation

Peter Brundrett
Principal Program Manager, Windows Kernel Team
Microsoft Corporation
Previous releases

- Windows Vista SP1 for x64 (2008)

New releases

- Windows Server 2008 R2 for x64 and Intel® Itanium®-based Platform (2009)
- Windows 7 (2009)

64-bit Windows versions only
Windows System Startup

Optimizing Boot

- System boot from large capacity hard drives
  - New storage devices > 2.2TB
- Pre-operating system software verification
  - Authenticoode signatures for firmware modules
- Enhance network protocols for deployment
  - IPv6 and network security
- Great performance with a modern look
  - Fast boot and resume response
  - High resolution graphics
Microsoft is committed to UEFI

- UEFI complements the transition to 64-bit computing
- Development of new firmware-related features will be on UEFI platforms first
  - Consider BIOS support where it makes sense

Call to Action: *Build UEFI platforms!*
- Write UEFI drivers for boot devices

Additional information
- Windows Hardware Developer Central
- [http://www.microsoft.com/whdc](http://www.microsoft.com/whdc)
- UEFI Support and Requirements for Windows
Summary

• UEFI is an industry standard with advanced firmware services enabling a stable platform foundation for richer OS Capabilities

• Industry leaders are using UEFI’s rich environment and delivering innovative solutions

• Utilize UEFI full potential - Build Class 2/3 UEFI Systems!

• Make use of the rich UEFI community resources
Q&A
Additional resources on UEFI:

• Other UEFI Sessions – Next slide
• Visit UEFI Booth #136
• More web based info:
  – OS Web links:
    • Link to Microsoft UEFI Support and Requirements:  [http://www.microsoft.com/whdc/system/platform/firmware/uefireg.mspx](http://www.microsoft.com/whdc/system/platform/firmware/uefireg.mspx)
    • Red hat link:  [https://fedoraproject.org/wiki/Features/EFI](https://fedoraproject.org/wiki/Features/EFI)
  – Whitepaper “Installing UEFI-based Microsoft Windows Vista SP1* (x64) on HP EliteBook and Compaq Notebook PCs” on [www.hp.com](http://www.hp.com)
## IDF 2009 UEFI Sessions

<table>
<thead>
<tr>
<th>EFI#</th>
<th>Company</th>
<th>Description</th>
<th>Time</th>
<th>RM</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>P001</td>
<td>Dell, HP, IBM, Intel, Microsoft</td>
<td>Using UEFI as the Foundation for Innovation</td>
<td>10:15</td>
<td>2005</td>
<td>T</td>
</tr>
<tr>
<td>S005</td>
<td>Phoenix, Intel</td>
<td>Transitioning the Plug-In Industry from Legacy to UEFI: Real World Cases</td>
<td>14:40</td>
<td>2002</td>
<td>Th</td>
</tr>
<tr>
<td>Q001</td>
<td>Intel, All</td>
<td>UEFI Q &amp; A session</td>
<td>15:40</td>
<td>2002</td>
<td>Th</td>
</tr>
</tbody>
</table>
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
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, Xeon 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.
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.
Backup Slides
Class break down back ground

- Background on Legacy
- UEFI (Unified Extensible Firmware Interface) firmware based deployment is expected to cross 50% of worldwide IA units by 2010
- Many of these platforms use UEFI for pre-boot, but perform OS boot through legacy support using CSMs (Compatibility Support Module).
- In many cases, the CSM boot support is the only boot option available on the platform.
- This has created a misleading impression that UEFI is not as pervasive in the industry as it actually is.

- Benefit of Exposing UEFI Interfaces
- The addition of a setup option to expose UEFI interfaces can provide the following benefits
  - UEFI allows innovation in the pre-boot environment
    - Custom enhanced user experience applications
    - Custom system management applications
    - Enhanced software test and diagnostic applications
    - Advanced system recovery utilities
  - Feature support:
    - Native x64 support
    - GPT partitioning (allows disk access beyond the 2 TB boundary
    - Modular support of technologies (security, networking, IPV6*)
  - Boot of UEFI supported OS’s
  - Customer interest in capability expansion through UEFI features
  - * IPV6 represents a technology currently under development and not currently (August 2009) available