Notebook Advancements for Unified Extensible Firmware Interface (UEFI) Pre-boot Productivity

Chenhao Xia , Technical Marketing Engineer, Intel
Kangkang Shen, Executive Vice President, Byosoft
Dong Wei, Distinguished Technologist, HP

EFIS002

Agenda

- **Overview of UEFI Pre-Boot Applications**
- **UEFI-based HP Innovations for Notebooks**
- **Byosoft Innovations for UEFI Pre-boot**
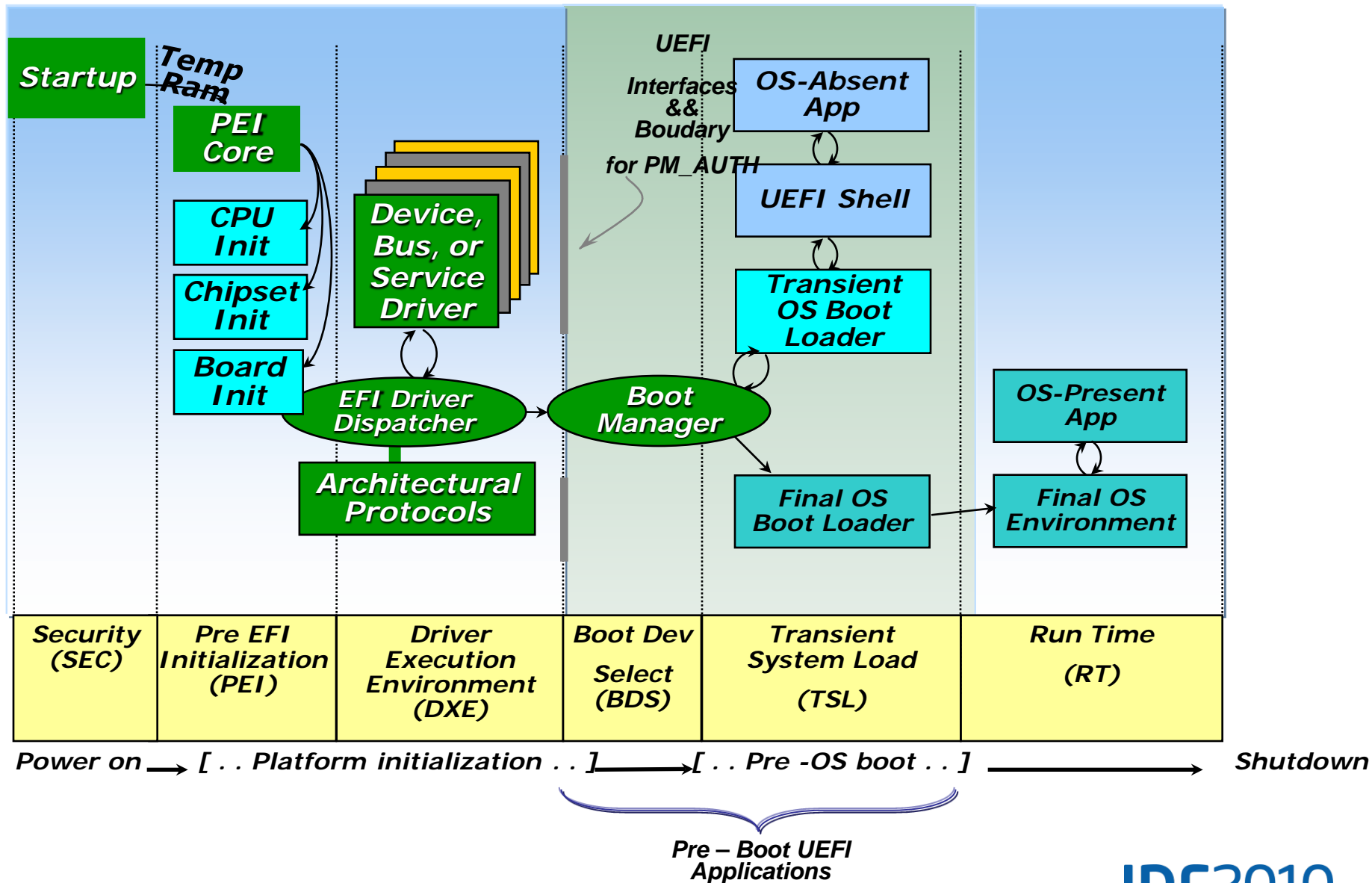
Agenda

- **Overview of UEFI Pre-Boot Applications**
- UEFI-based HP Innovations for Notebooks
- Byosoft Innovations for UEFI Pre-boot
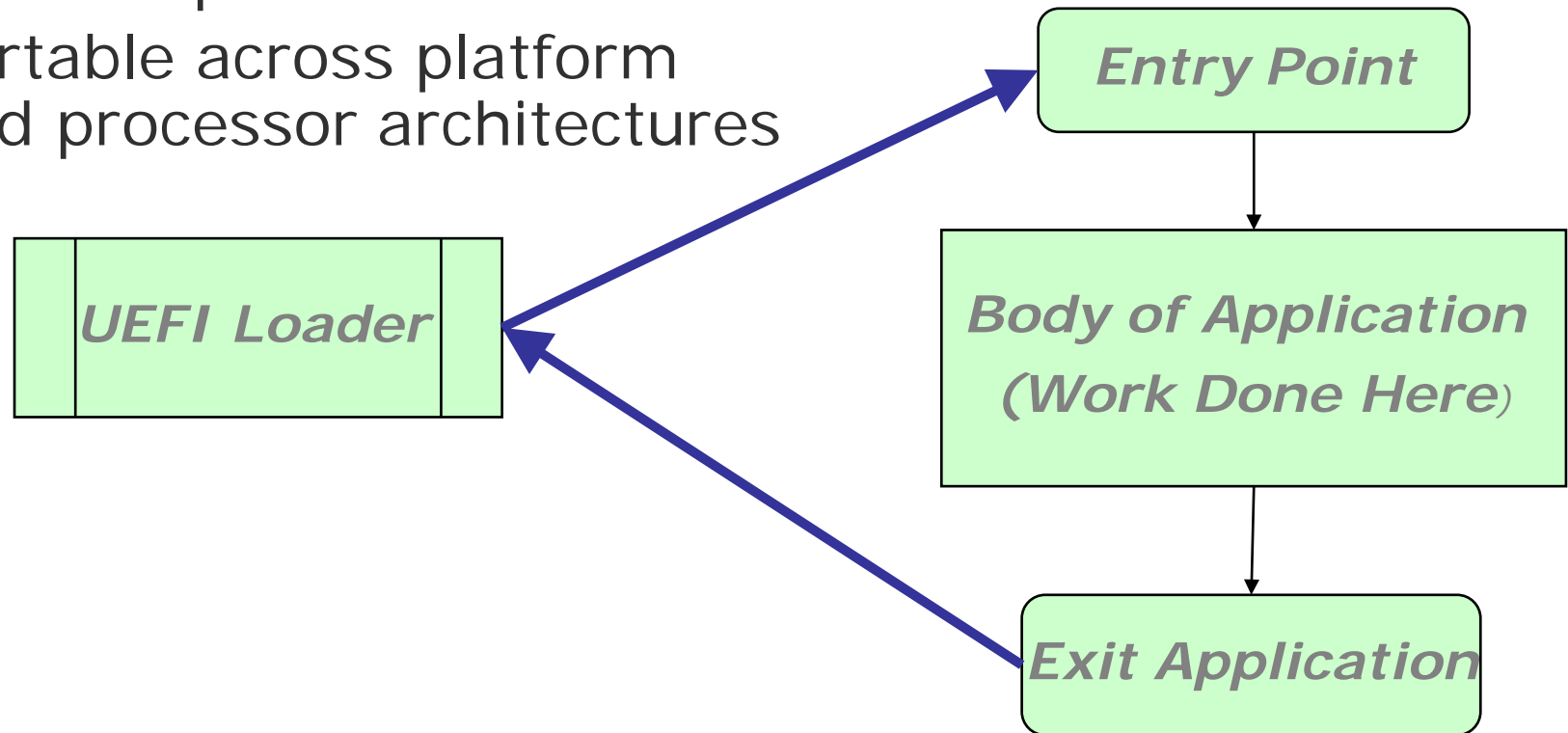
What is an UEFI Application?

- An UEFI Loadable Image
  - Loaded by UEFI loader just like UEFI drivers
  - Does not register protocols like UEFI drivers do
  - Consumes protocols
  - Typically user driven (exits when task completed)
  - Same set of interfaces available as drivers have
- Can be used for
  - Platform diagnostics
  - Factory diagnostics
  - Utilities
  - Driver prototyping
  - 'Platform' applications

IDF2010
INTEL DEVELOPER FORUM

Boot Execution Time Line

Security (SEC)	Pre EFI Initialization (PEI)	Driver Execution Environment (DXE)	Boot Dev Select (BDS)	Transient System Load (TSL)	Run Time (RT)

Power on → [. . Platform initialization . .] → [. . Pre -OS boot . .] → Shutdown

Pre – Boot UEFI Applications

UEFI Pre-boot Application Execution

- Abstractly Extend the Firmware without hardware or OS dependence
- Portable across platform and processor architectures

```
                          Entry Point
                               |
                               v
    UEFI Loader        Body of Application
                       (Work Done Here)
                               |
                               v
                       Exit Application
```

Pre-Boot UEFI Applications Extend Firmware

IDF2010
INTEL DEVELOPER FORUM

Agenda

- **Overview of UEFI Pre-Boot Applications**
- **UEFI-based HP Innovations for Notebooks**
- **Byosoft Innovations for UEFI Pre-boot**

UEFI-based HP Innovations for Notebooks

Dong Wei – HP Distinguished Technologist
April 14, 2010

HP Innovations for Notebooks based on UEFI Technology

- HP Diagnostics

- HP QuickLook

- HP DayStarter

Enhanced Diagnostics

- Based on the UEFI Technology
- DIMM fault isolation
- Hard drive simultaneous test
- Concurrent memory, hard drive and batteries test
- Improve test coverage, optimize test cycles

HP QuickLook

- Technology that lets you access your Outlook data in seconds when your notebook is off

- With HP QuickLook 3, you can edit your e-mail, calendar, contacts and tasks

  - Automatically synchronized the next time you start your computer.

  - Boasts updated security features, can authenticate your identity using the same password or fingerprint reader you use to log on to Microsoft® Windows®.

  - Can specify the frequency at which data is captured, the type of data that is captured (e-mail, calendar, contacts and tasks), and the range of data that is captured.

THE
COMPUTER IS
PERSONAL
AGAIN·

HP QuickLook (Cont.)

WORK FASTER AND SIMPLIFY YOUR LIFE WITH HP QUICKLOOK 3.

Three-month rolling calendar

Current time and date

E-mail, calendar, contact and task creation and editing

HP QuickLook 3

3:58 PM
Monday, May 11, 2009

Today - Admin

April 2009

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May 2009

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

June 2009

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Calendar

11:00 - 12:00   Lunch with Clients (TBD)
3:00 - 4:00   Staff Meeting (Conference Room 123)

Upcoming calendar events

Tasks

Today   Call IT Repair
May 13   Send HR notification
May 15   Send Payroll Check
May 29   Rebuild Lab

Current tasks

Detail information

3:00 - 4:00 PM
Staff Meeting

Location: Conference Room 123
Organizer: Smith, John

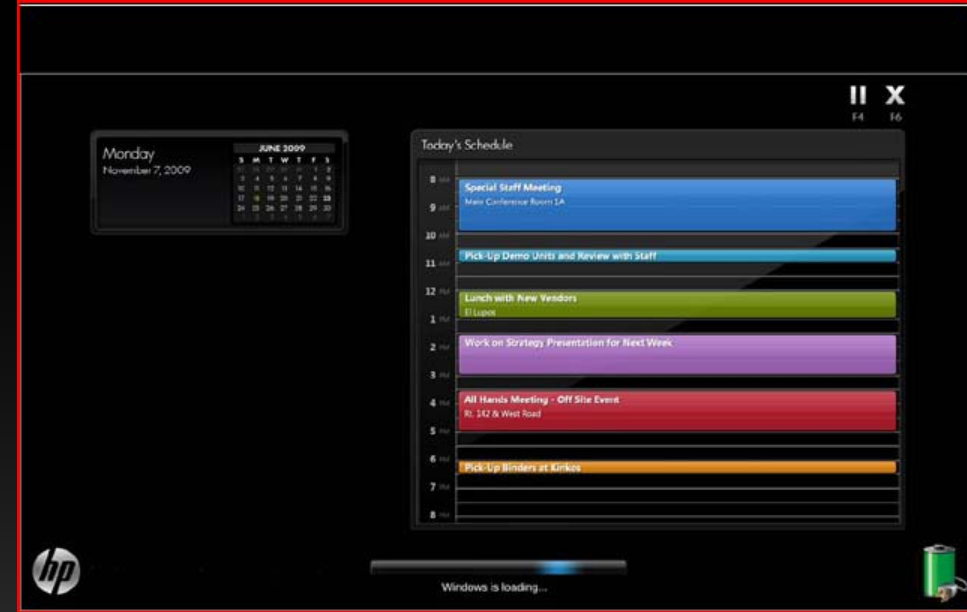Please attend this staff meeting to discuss the state of the business. Agenda to follow.

Easy navigation
It's easy to access and edit information with HP QuickLook 3. When you push the HP QuickLook button, the Today page opens. It displays a three-month calendar, upcoming calendar events and your active tasks, along with the current date and time. You can then use intuitive icons to navigate to and edit more detailed information, including e-mail messages, calendar entries, contacts and tasks.

HP DayStarter

- Integral part of HP QuickLook 3.2 and above

- A new feature on the new HP commercial EliteBook and ProBook notebooks (selected models at first launch)

- Allow user to personalized information while the computer is booting

- Displays the following information:
  - Calendar summary
  - Battery icon
  - Windows status
  - Pause and escape buttons

- Supported in the HP Mobile Framework UEFI Codebase

See eWeek DayStarter Artical:

http://www.eweek.com/c/a/IT-Infrastructure/HP-Unveils-New-ProBook-Notebooks-and-EliteBook-Business-Tablets-257234/

THE COMPUTER IS PERSONAL AGAIN.

OutLook PIugins for HP QuickLook

HP QuickLook icons

When HP QuickLook is installed, the icons shown and described in the following table are displayed on the Outlook toolbar.

Icon	Action
HP QuickLook Preferences	Configures HP QuickLook preferences.
HP QuickLook Capture	Manually initiates HP QuickLook information capture.
HP DayStarter icon	Configures HP DayStarter preferences.

Setting HP DayStarter preferences

To select HP DayStarter preferences, follow these steps:

1. Click the **HP DayStarter** icon on the Outlook toolbar.
2. The following note is displayed:

   NOTE: Activation of HP DayStarter displays JPEG based images during system startup. These images may include personal calendar and event details that could be seen by other users of this system in a multi-user environment.

3. Click **Yes**.
4. Select the 12-hour calendar time period to be displayed when the computer restarts.
5. To save your changes, click **OK**.

UEFI enables faster and easier innovations

Agenda

- **Overview of UEFI Pre-Boot Applications**
- **UEFI-based HP Innovations for Notebooks**
- **Byosoft Innovations for UEFI Pre-boot**

UEFI Pre-boot Application Development

- Use EDK/EDKII as development kit
- Development process as same as UEFI drivers
- Use UEFI Boot Services to implement functions
- Rich libraries support
  - EDK/EDKII libs
  - Other venders, Byosoft GUI , Security libs
- Use "C" as main development language
  - Engineers pool is cheaper
  - Reuse C source code resource

Easy To Develop – Byosoft

Byosoft UEFI Pre-boot Application Examples

- Manufacture Tool
  - *Ghost-like Tool*
  - *Flash Tool*
  - *Hide partition Tool*
- Security Application
  - *Pre-boot Anti-virus*
- Value-Added
  - *Pre-boot AD*

- Debug Utility
  - UEFI Handle Dump
  - Driver Stack Dump
  - PCI/Memory Space Dump
- DOS Replacement Tool
  - HDD Partition
  - File management
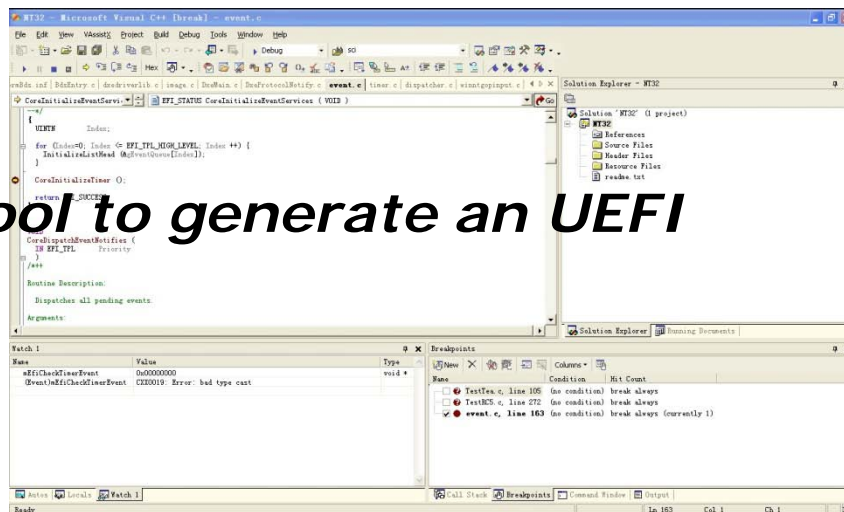
Rich Pre-boot Applications Accumulation — Byosoft

UEFI Pre-boot Application - Build Description File

Set MODULE_TYPE in your module's .INF file to UEFI_APPLICATION.

```
[Defines]
  INF_VERSION        = 0x00010005
  BASE_NAME          = MyApplication
  FILE_GUID          = 10C75C00-30 . . .
  MODULE_TYPE        = UEFI_APPLICATION
  VERSION_STRING     = 1.0
  ENTRY_POINT        = MyApplicationMain
```

This will cause the build tool to generate an UEFI Application image.

UEFI Pre-boot Application Development - Tips

- The UEFI Application runs on a UEFI Task Priority set at TPL_APPLICATION, which is the lowest priority. It may be interrupted by some DXE drivers.

- Do NOT use any of PI defined protocols because PI is only designed to be used by UEFI firmware itself

- If you are implementing an OS loader, DO NOT call any of UEFI boot services after the *ExitBootServices* function is invoked

- Always allocate memory which is boot service attribute

- By default the DXE dispatcher will not dispatch this type of module

Byosoft Pre-boot Innovation: Pre-boot AD

- Great Innovation in UEFI pre-boot applications
  - Play video and audio during system boot
    - Can be used to show advertisement, animation and other user selected video to bring great user experiences in notebook systems
  - User customizable
    - Provide edit utility to change the pre-boot video
- Integrated into Byosoft desktop and mobile product line
- Implemented as a set of UEFI pre-boot applications
  - Pre-boot Decoder
  - Pre-boot video player
- Support various multimedia formats
    - Native support AVI format
    - Provide video format convert tool support more multimedia formats

A Great Place to Innovate – Byosoft

BYOSOFT
百 敖 软 件

IDF2010
INTEL DEVELOPER FORUM

Byosoft UEFI Pre-boot Example Pre-boot AD Technology Cont.

PC boot Comparison

With Pre-boot AD VS Without Pre-boot AD

Summary

- UEFI leaves ample room for pre-boot applications

- Leading notebook provider HP has taken advantage of UEFI and delivered pre-boot applications on its new models

- UEFI technology is maturing and ready to use, but the room for innovation is unlimited.

- IBVs have worked on UEFI for many years and their year's accumulation can be utilized by you right now.

Next Steps

- Using UEFI environment to host your pre-boot applications

- Differentiate your mobile products through UEFI pre-boot applications

- Contact Intel and IBVs for off the shelf pre-boot applications

- Contact IBVs for customized pre-boot applications

  kshen@byosoft.com.cn

UEFI enables faster and easier innovations

IDF2010
INTEL DEVELOPER FORUM

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications and Implementation sites: www.tianocore.org, www.uefi.org, www.intel.com/technology/efi
  - Whitepaper: "Installing UEFI-based Microsoft Windows Vista SP1* (x64) on HP EliteBook and Compaq Notebook PCs" on www.hp.com
  - Whitepaper: "QuickLook-3", http://www.hp.com/sbso/solutions/pc_expertise/professional_innovations/quicklook-3.pdf
- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress
- UEFI Plugfest Event at Intel in Dupont Washington, June 22-25, 2010 www.uefi.org or email: laurie.jarlstrom@intel.com

IDF 2010 UEFI Spring Sessions April 14

EFI#	Company	Description	Time	RM
S001 ✔	Intel, IBM, HP	Using the Latest EFI Development Kit (EDK II) for UEFI Advanced Development and Innovation	11:10	302AB
S002 ✔	Intel, HP, Byosoft	Notebook Advancements for Unified Extensible Firmware Interface (UEFI) for Pre-boot Productivity	13:00	302AB
S003	Intel, Byosoft	Unified Extensible Firmware Interface (UEFI): Best Platform Security Practices	14:00	302AB
S004	Intel, Microsoft, Insyde	UEFI Fast Boot for Microsoft* Windows* 7 : Fast Boot Without Compromising your BIOS	15:00	302AB
S005	Intel, Inspur, Insyde	UEFI Firmware Solutions for Enterprise Servers: A Case Study in 8-way Processor Support	16:00	302AB

✓ *DONE*

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/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

IDF2010
INTEL DEVELOPER FORUM

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

IDF2010
INTEL DEVELOPER FORUM

Q&A

IDF2010
INTEL DEVELOPER FORUM

Legal Disclaimer

IDF2010
INTEL DEVELOPER FORUM

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first 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. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; 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; defects or disruptions in the supply of materials or resources; 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; product mix and pricing; 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; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; the timing and execution of the manufacturing ramp and associated costs; and capacity utilization; . 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 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 the timing of closing of acquisitions and divestitures. 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. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting our ability to design our products, or requiring other remedies such as compulsory licensing of intellectual property. 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.

Rev. 1/14/10