UEFI Fast Boot for Microsoft* Windows* 7: Fast Boot Without Compromising your BIOS

Yuanyuan Xing, Technical Marketing Engineer, Intel
Aven Chuang, Senior VP & GM, Insyde Software
Mark Svancarek, Principal Program Manager, Microsoft

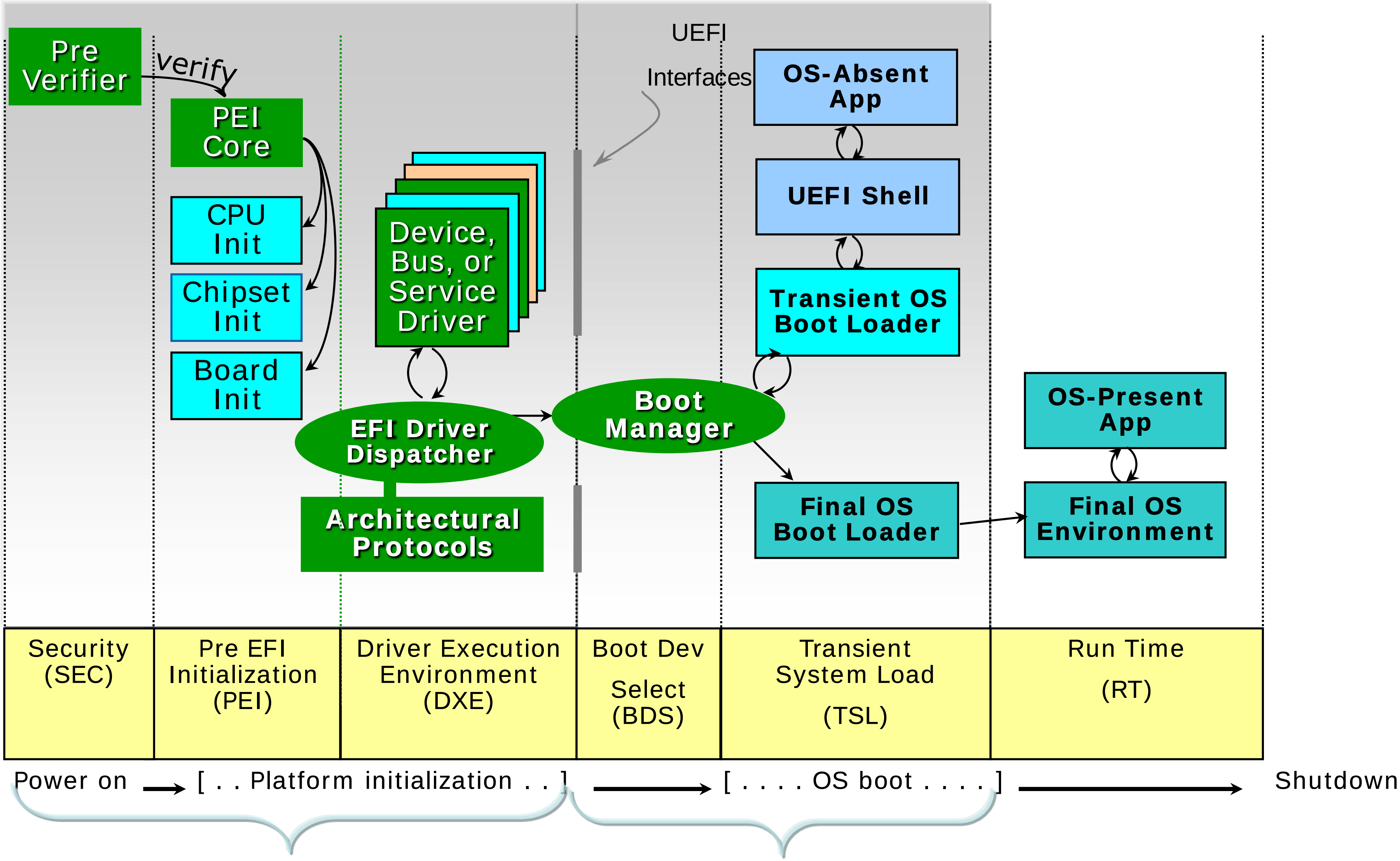
EFIS004

Sponsors of Tomorrow.™ intel™

Agenda

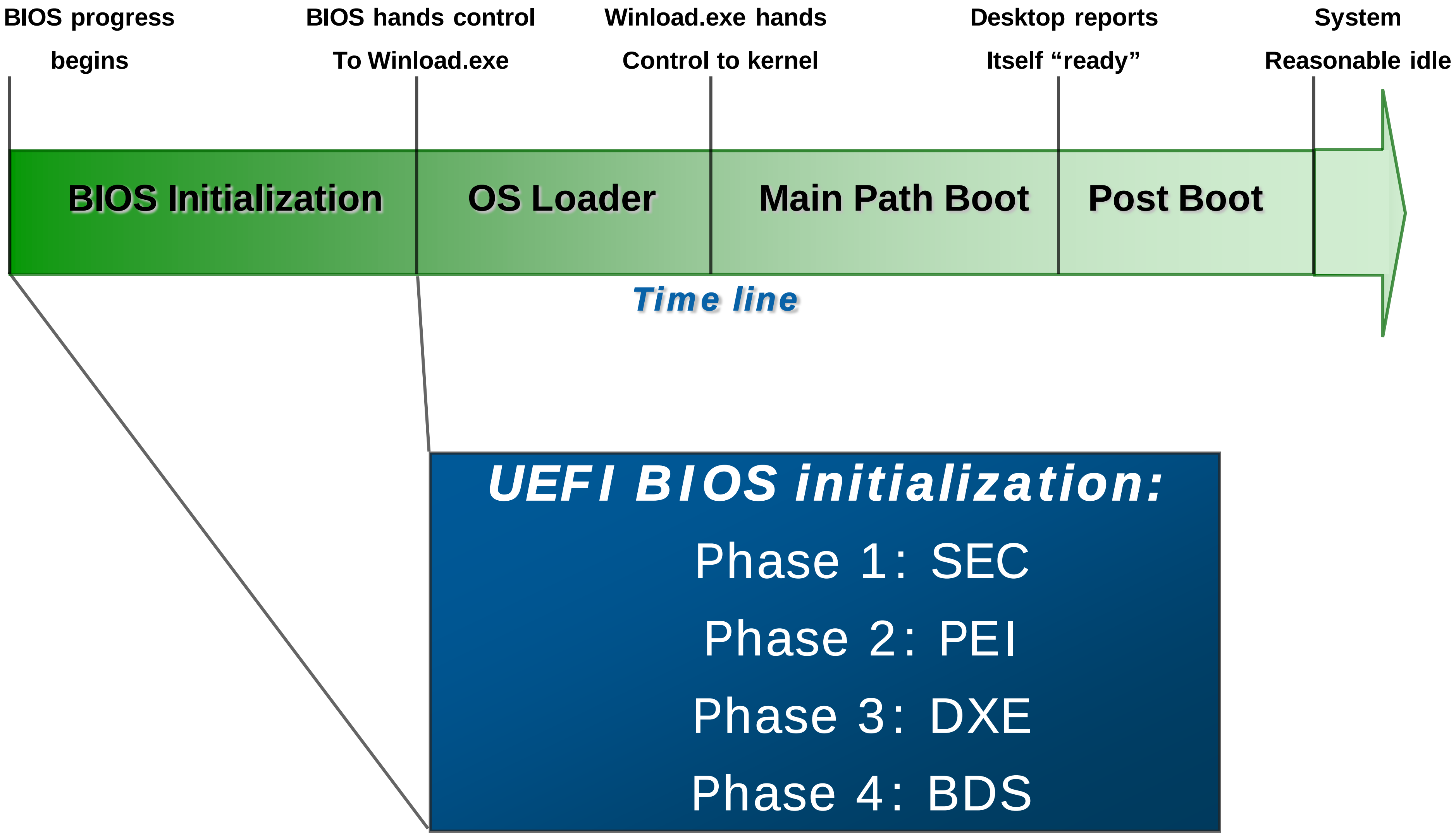
- Overview of boot time
- Performance improvements for boot times
- Demo
- Why fast POST for Windows* 7
- Other considerations for Windows 7

Overall View of Boot Time Line



IDF2010 INTEL DEVELOPER FORUM

Overview of Boot Time



BIOS progress begins

BIOS hands control To Winload.exe

Winload.exe hands Control to kernel

Desktop reports Itself “ready”

System Reasonable idle

BIOS Initialization

OS Loader

Main Path Boot

Post Boot

Time line

UEFI BIOS initialization:

Phase 1: SEC

Phase 2: PEI

Phase 3: DXE

Phase 4: BDS

Overview of Boot Time

- 4 UEFI BIOS Initialization phases:
  - **SEC** (Security) phase: Pre-RAM code handles CPU initialization to create temporary stack in CPU cache.
  - **PEI** (Pre-EFI initialization) phase: finishes CPU initialization, discovers the DRAM, and determines boot mode (cold boot, S3, S4)
  - **DXE** (Driver Execution Environment) phase. Loads drivers that initialize the rest of system hardware.
  - **BDS** (Boot Device Selection) phase. Finds boot devices, loads the OS, and passes control over to the OS.

Agenda

✓ Overview of boot time

- Performance improvements for boot times
- Demo
- Why fast POST for Windows* 7
- Other considerations for Windows 7

Overview of Fast Boot Solutions

BIOS POST time can be improved in three ways:

1. Remove drivers, or
2. Fine tune drivers, or
3. Hide drivers when not used

(Note: A software tool can be used to do the analysis the consumed time of your drivers)

Example of Analyzed Driver Time

SEC Phase Duration	:	317(ms)
PEI Phase Duration	:	148(ms)
DXE Phase Duration	:	387(ms)
BDS Phase Duration	:	775(ms)
Total Duratio	:	1627(ms)

Name	Duration time(ms)
HiiDatabase:	10
Crc32SectionExtract:	9
FwBlockService:	2
FtwLite:	2
Variable:	11
SetupUtility:	2
MiscSubclass:	8
MpCpu:	94
SmbiosMemory:	61
IsaBus:	1
LightPciBusPciBus:	20
SataController:	146
ConSplitter:	3
BiosVideo:	273
SmmBase:	30
PchInitDxe:	6

Name	*Duration time(ms)*
AcpiPlatform:	*2*
LegacyBios:	*38*
Ahci:	*66*
SmmRuntime:	*1*
SmmFwBlockService:	*1*
SmmFtw:	*49*
PowerManagement2:	*2*
SmmPlatform:	*2*
Ihisi:	*1*
OemInt15Callback:	*1*
	:
	:
	:
	:
	:
	:
	:

Manage Drivers After the Analysis

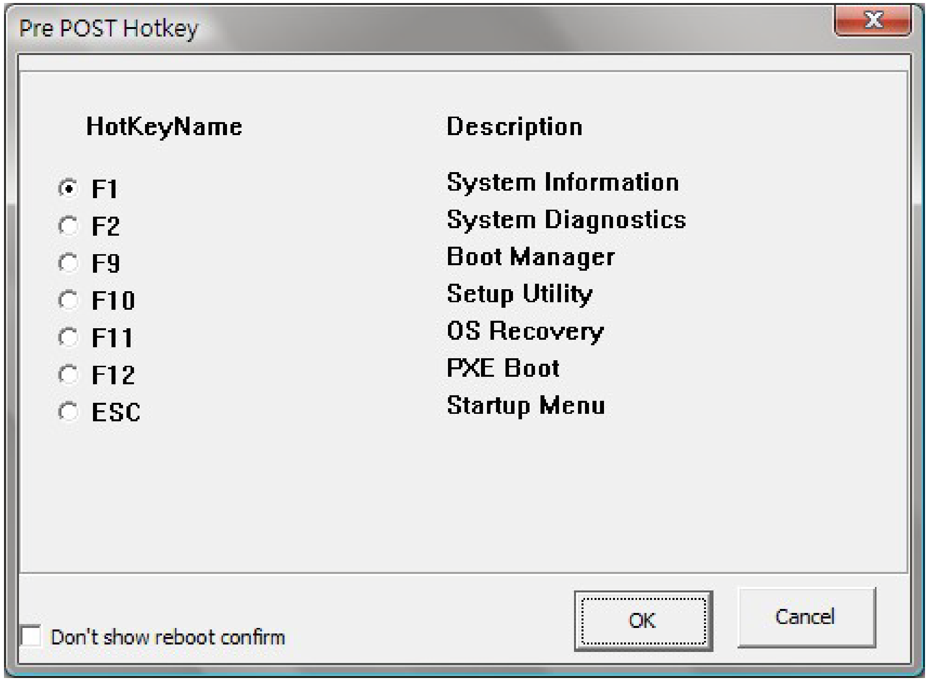
Module	Customer Decision
Module 1	Must have
Module 2	Removed
Module 3	Must have
Module 4	Removed
Module 5	Hidden
Module 6	Hidden
Module 7	Hidden
Module 8	Removed
Module 9	Must have
…	…

- Analyze the list of modules for customers to decide whether the features should be kept, removed, or hidden.
- The "Hidden" items don't run unless:
  - First boot after configuration changed
  - Previous boot fails
  - Pre-Post hotkeys pressed
  - Triggered by windows application

Trigger for Special Purpose

- EC Support
  - EC codes to be defined for users to go to the user interface in POST
  - While pressing Power button, if a hotkey is also pressed (e.g. F10), BIOS will boot to SCU or the defined page.

- Windows application
  - *The user can select where to reboot to.*


Pre POST Hotkey

HotKeyName	Description
● F1	System Information
○ F2	System Diagnostics
○ F9	Boot Manager
○ F10	Setup Utility
○ F11	OS Recovery
○ F12	PXE Boot
○ ESC	Startup Menu

□ Don't show reboot confirm

Performance Improvement

Disk Type	SSD		HDD	
Blink Boot (Seamless AHCI + Smart Boot)	On	Off	On	Off
IRU	1.692	3.021	1.912	3.314
BIOS POST (Volecity)	2.75	4.11	3.63	5.06

Performance Improvements on Actual OEM platform

(more “must have” items stay here)

Disk Type	SSD		HDD	
Smart Boot	On	Off	On	Off
IRU	2.068	3.021	2.313	3.314
BIOS POST (Velocity)	3.25	4.11	4.16	5.06

Agenda

✓ Overview of boot time

✓ Performance improvements

- Demo
- Why fast POST for Windows* 7
- Other considerations for Windows 7

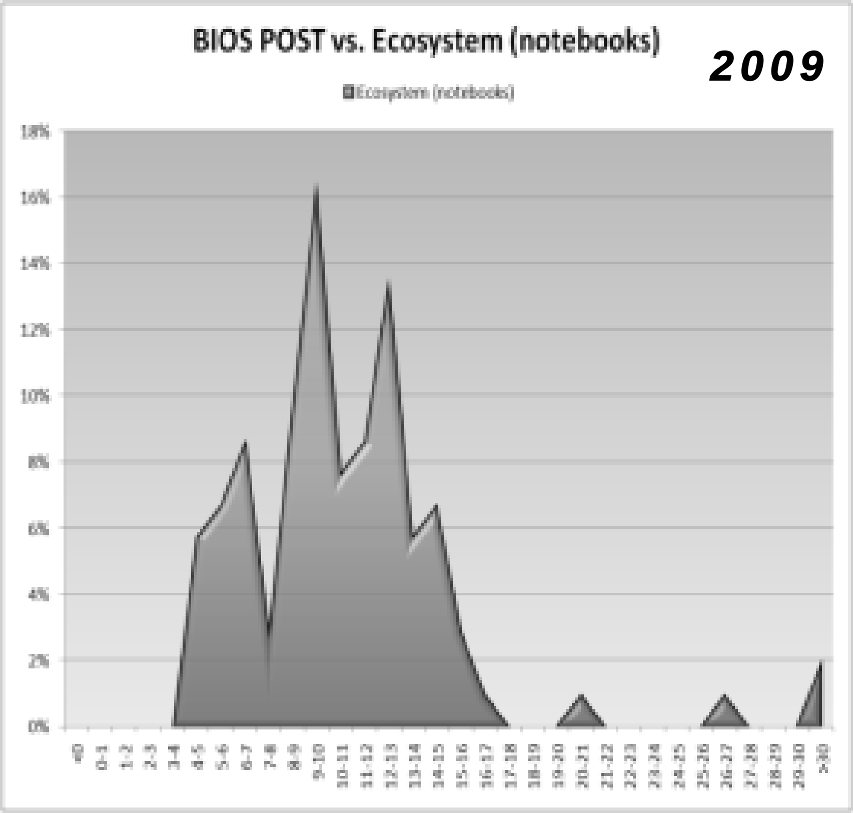
Agenda

- ✓ Overview of boot time
- ✓ Performance improvements
- ✓ Sample results
- ✓ Demo
- Why fast POST for Windows* 7
- Other considerations for Windows 7

Why fast POST for Windows® 7

What we said at IDF in September 2009

- *In a recent audit of Windows 7 notebooks, 34% booted in 35 sec or less*
- *Not including post times*
- *Since Windows 7 boot times are faster than Windows Vista SP1 on any HW, long POST times are more noticeable and undesirable for end users*

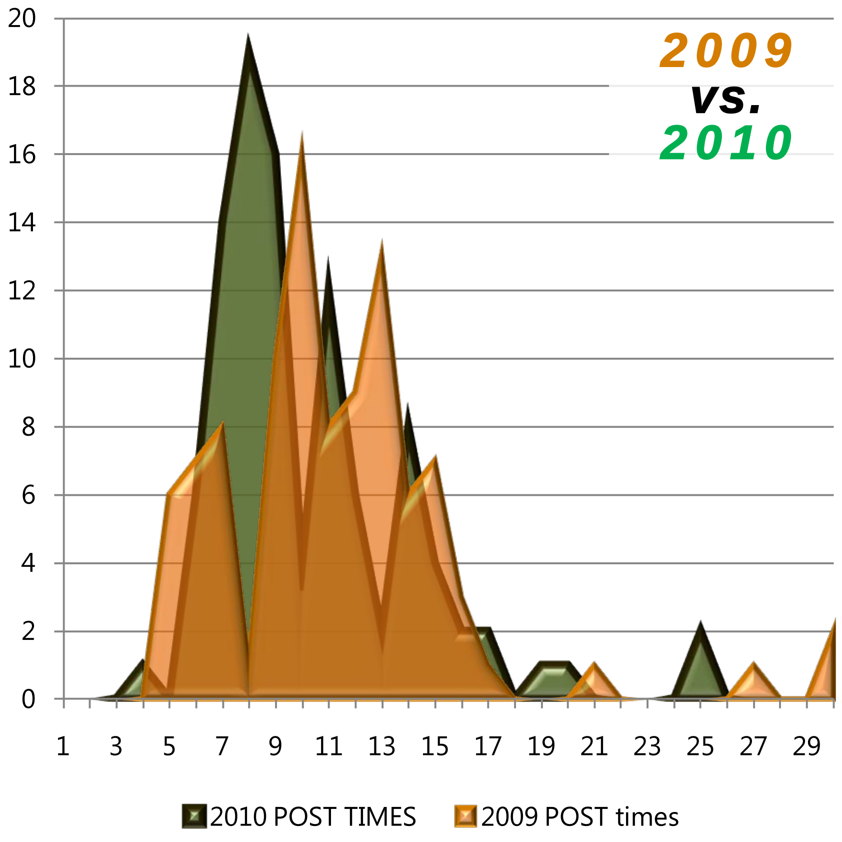


2009

“Source: Microsoft Windows OEM Engineering Services”

Why fast POST for Windows® 7: Update

- Fast POST is becoming mainstream for Windows 7 machines
  - Median POST time 3 sec faster than Windows Vista (11 sec → 8 sec)
- But some very slow POST still remain



“Source: Microsoft Windows Ecosystem Engineering”

Agenda

- ✓ Overview of boot time
- ✓ Performance improvements
- ✓ Demo
- ✓ Why fast POST for Windows* 7
- Other considerations for Windows 7

Other Windows® 7 Considerations

- Baseline to prevent regressions
  - Use Velocity Tools or Windows Logo Kit to baseline firmware times during power transitions
  - Especially important if you did not have aggressive targets for Windows® Vista®
  - Verify that you do not have dependencies on undocumented Windows behavior
    - Example: restoring MTRRs for each CPU after S3 resume
      - Adds ~400 milliseconds
      - Also impacts time to synchronize the processor TSCs (new for Windows® 7)

Other Windows® 7 Considerations

- Keep BIOS CSM compatibility layer small
  - Windows 7 does not require Int13 support for storage
    - Use UEFI interface instead
  - Int10 still required
  - Usually possible to initialize the video BIOS without the CSM
    - Int10 still required, but not during POST
    - The video BIOS must be in the C0000 segment and a real-mode IDT at physical address 0x0

Other Windows® 7 Considerations

- 64-bit OS & 4 GB
  - 4 GB RAM machines became common in Windows Vista® SP1 timeframe
  - 64-bit OS required to support 4 GB RAM
  - Verify that there are no issues accessing 64-bit ISOs from CD-ROM or DVD
- Solid State Drive (SSD) compatibility
  - SSDs now becoming popular for both high-end and low-end machines with Windows 7
  - Verify that there are no race conditions or other compatibility problems
  - Verify both boot and hibernate use cases

Other Windows® 7 Considerations

- ACPI runtime firmware accessing memory from an AcpiReclaimMemory memory region
  - ACPI defines AcpiReclaimMemory as memory that can be reclaimed by OS after it copies memory out of it
    - Typically used by the platform for ACPI tables
  - Windows 7 does not currently reclaim this memory and does not currently verify that ACPI firmware does not attempt to access this memory

Other Windows® 7 Considerations

- Wrong device paths in EDD
  - Legacy BIOS provides a mechanism to know the physical path to a HDD
    - e.g., PCI Express* Bus/Device/Function, IDE controller, master
  - Windows 7 does not depend on this behavior
    - majority of Legacy BIOS implementations populated this information incorrectly.

Summary

- Since Windows® 7 boot times are much faster, Faster firmware POST times are required
- Faster POST improvements are achieved by Selecting the best performing hardware and reducing the POST time features
- Beware of other Windows 7 considerations
- UEFI by design can help improve on boot time performance

Next Steps

- Work with your BIOS teams to push for POST improvements
- Specify POST times to your ODMs
- Specify minimum hardware performance standards to your ODMs
- Make use of the latest UEFI and PI Specifications to help your design make improvements in boot times
- Download the Microsoft White paper: http://www.microsoft.com/whdc/system/platform/firmware/FirmwareEnhance_Win7.mspx.

Microsoft

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
  - Link to Microsoft UEFI Support and Requirements: http://www.microsoft.com/whdc/system/platform/firmware/uefireg.mspx
- 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

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 © 2010 Intel Corporation.

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