UEFI Boot Time Optimization Under Microsoft* Windows 7*

Mark Doran
Senior Principal Engineer, Intel

Kevin D. Davis
VP Client Chipset and Kernel Engineering, Insyde Software

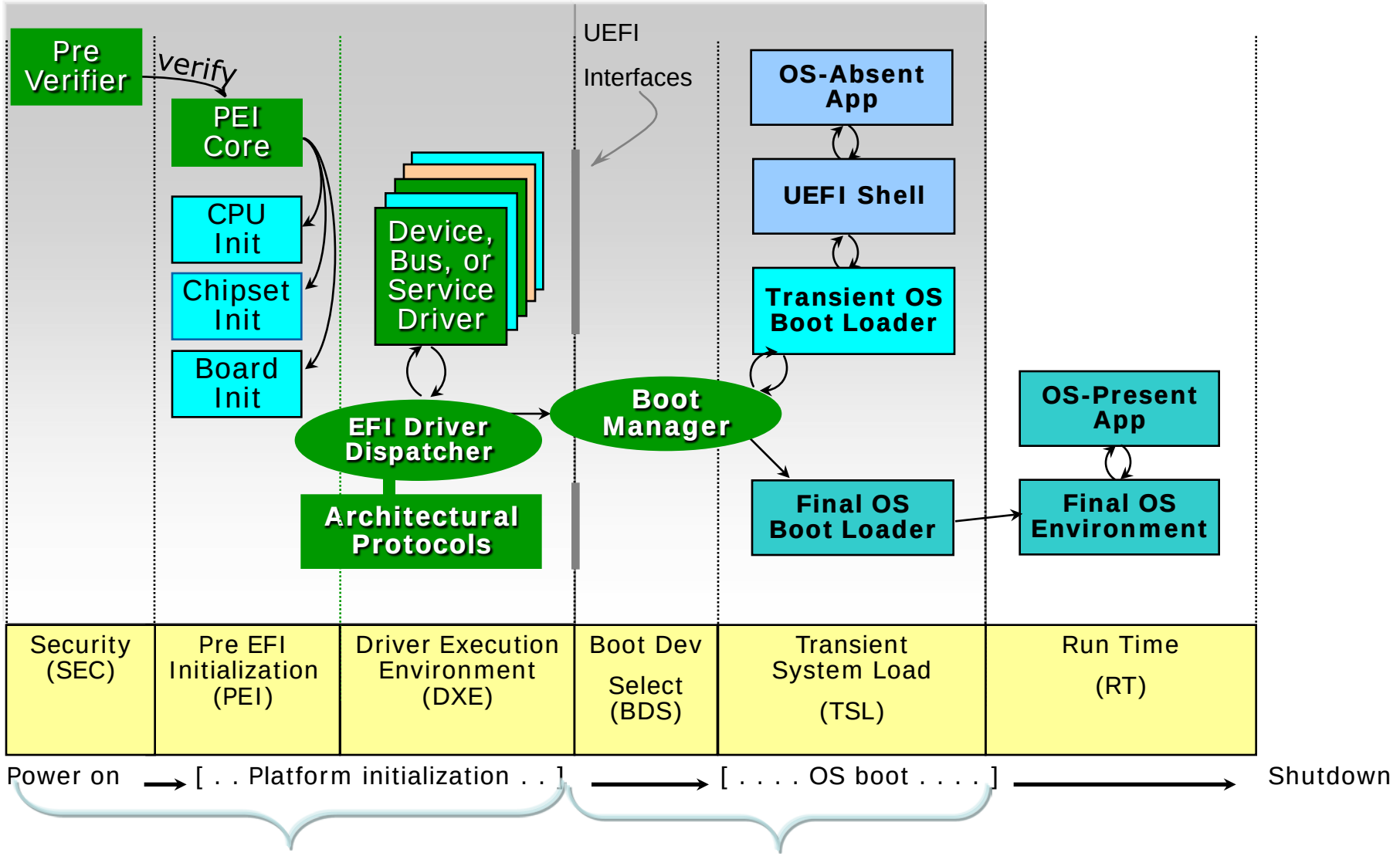
Mark Svancarek
Principal Program Manager, Microsoft Corporation

EFIS004

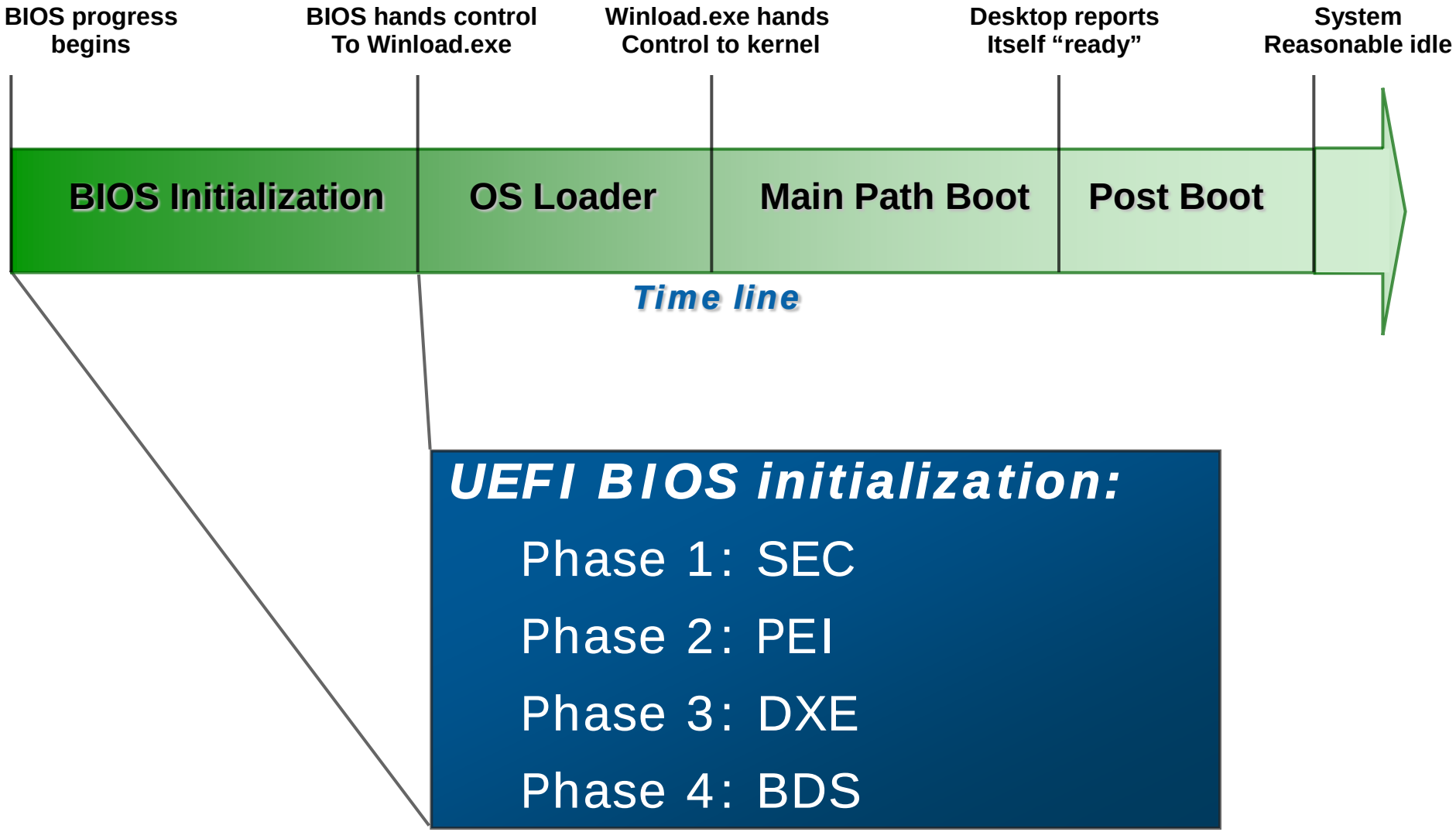
Agenda

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

Overall View of Boot Time Line



Overview of Boot Time



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

Typical UEFI BIOS Initialization Time

Intel® Mobile Platform with Intel® Core™ i7-920XM Processor Extreme Edition[1]	
SEC phase	1.638 s
PEI	2.647 s
DXE	1.296 s
BDS	3.139 s
Total Duration: 8.720 s[2]	

[1] Reference platform

[2] Using InsydeH2O BIOS*; Source - Insyde Software Corp

Performance Improvements

SEC phase:

- Aggregate all SEC and PEI drivers to 1 64Kb block of flash
  - All code must be in the processor's cache before enabling Non-Eviction Mode
- If code is outside NEM area, it is running extremely slow
- Set CPU throttling to min (max power)
- CPU microcode loading
  - Only 1 in system; no searching

Performance Improvements

PEI:

- Memory Init:
  - Don't clear memory to zero with code
  - Use hardware if available in memory controller
  - Or don't clear it at all, if no ECC req'd
- Skip Memory detection:
  - No SMBus SPD reads
  - Good for closed systems

Performance Improvements

DXE:

- DXE dispatcher tries to load and run DXE drivers in a round robin loop
  - Reduce dependencies to a minimum
  - Try to have drivers loaded in efficient order
  - a-priori
  - Don't hard-code drivers in a-priori file, unless absolutely necessary -- can only get it wrong

Performance Improvements

Other DXE improvements:

- Multi-threading:
  - UEFI drivers are re-entrant although not yet MP safe
  - Carefully assign discrete tasks to the APs during DXE
- Remove PS/2 devices:
  - Legacy devices are slow to respond
  - Use high-speed USB devices

Performance Improvements

Other DXE improvements:

- Legacy Option ROMs:
  - Originally designed to extend functionality of PC-AT systems with device-specific code
    - PXE UNDI, video, storage devices
  - Replaced by UEFI device drivers, and UEFI compliant Option ROMs
  - Don't initialize Legacy Option ROMs if you don't need the device

Use UEFI drivers instead

Performance Improvements

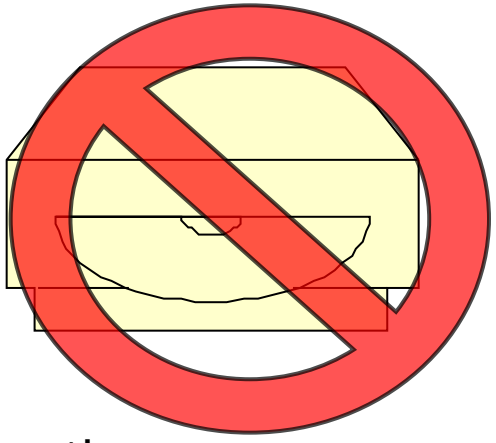
Other DXE improvements:

- Video:
  - Legacy video is extremely slow and time consuming to boot
  - Insist on Native UEFI video drivers
  - Use console redirection to avoid initializing video
- SATA channels:
  - Don’t initialize extra SATA channels
  - Let Windows* 7 do it

Performance Improvements

BDS phase:

- Use SSD instead of rotating media:
  - Rotating media is comparatively slow



- Pre-select the boot device:
  - No searching for devices -- It's too slow
    - Systems boot from same device 99%+ of the time
  - Cut this phase to almost nothing by booting from a single pre-determined device

Performance Improvements

Other overall improvements:

- Compiler optimizations:
  - UEFI code is written in C
  - Make sure max speed is enabled

- Embedded Controller (EC)
  - Slow device -- Minimize usage
  - SPI flash with UEFI BIOS behind EC – very slow
  - Direct SPI Flash off SouthBridge

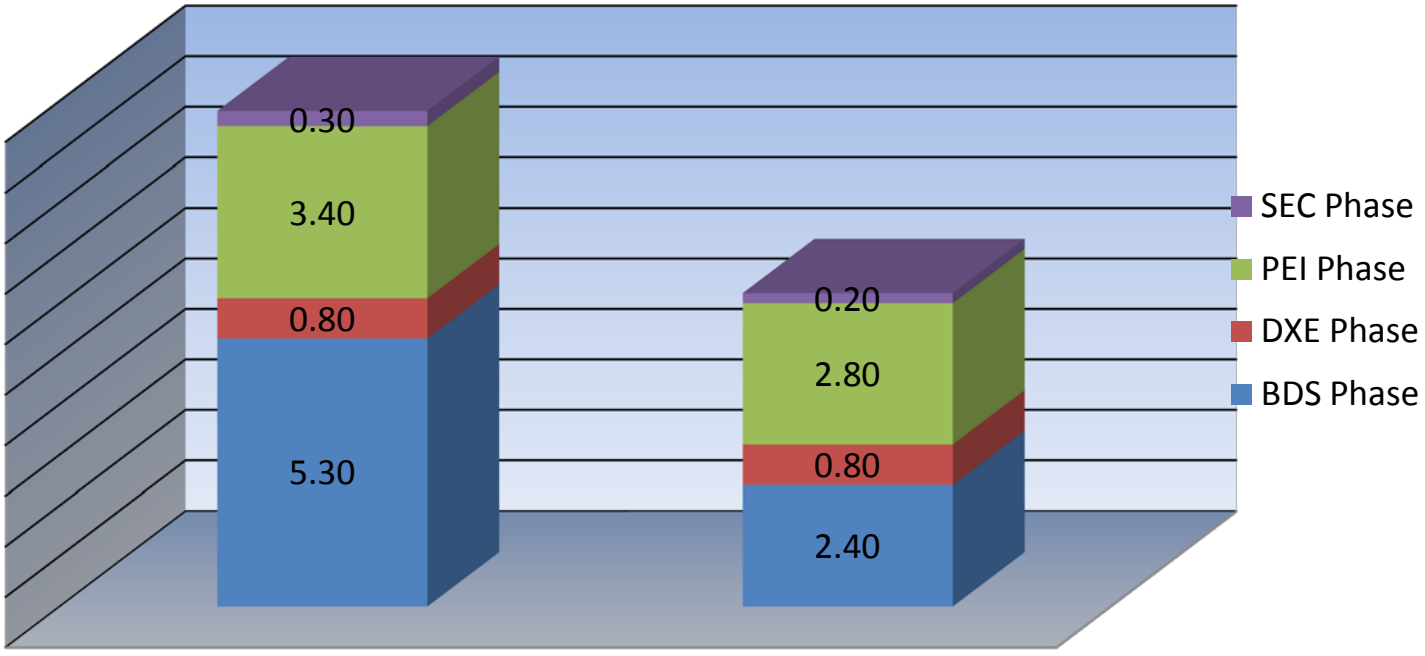
Agenda

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

Customer Platform Improvements

UEFI BIOS optimization - InsydeH2O customer BIOS

Task	Before (sec)	After (sec)
SEC Phase	0.30	0.20
PEI Phase	3.40	2.80
DXE Phase	0.80	0.80
BDS Phase	5.30	2.40
Total	**9.80**	**6.20**

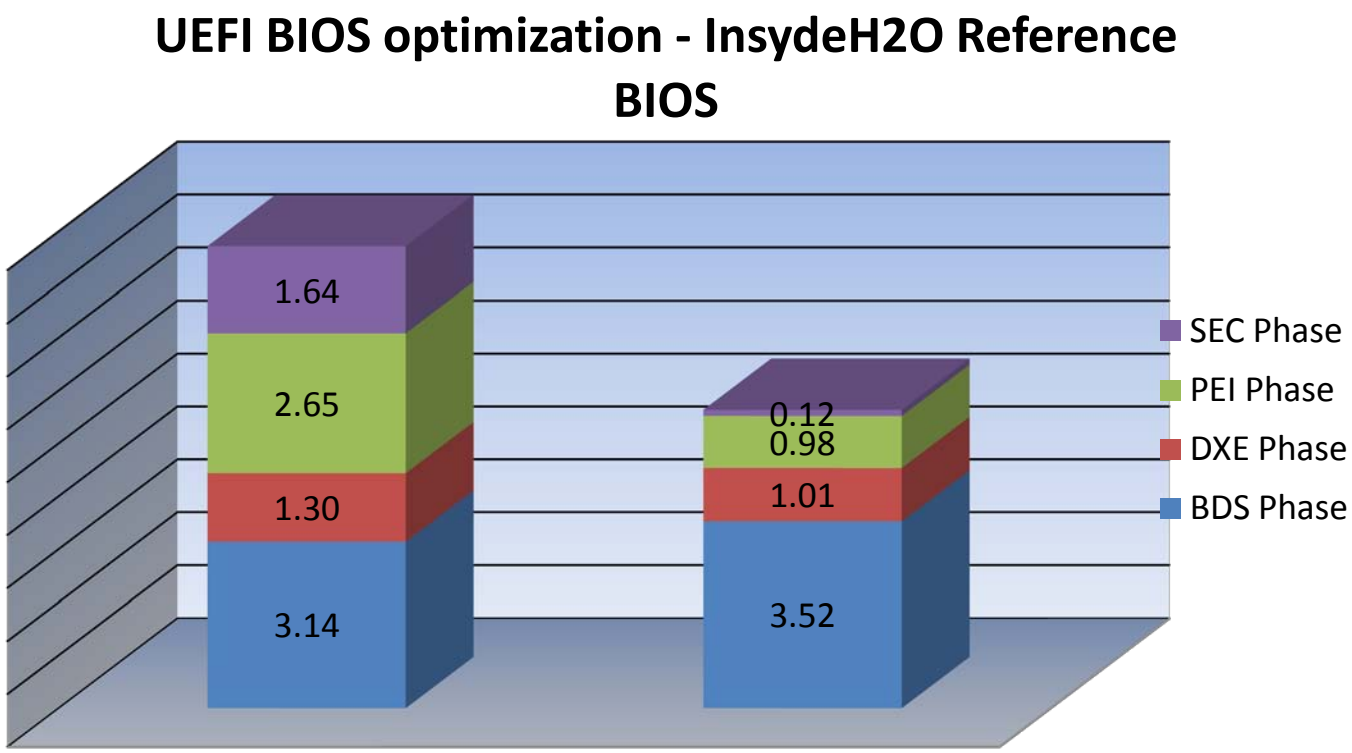


Source: Insyde software, Mobile Reference platform

- Improvements made in all phases of POST
- 25% reduction in boot time.
- System still passes Microsoft WLK 1.4 tests

Reference board improvements

Task	Before (sec)	After (sec)
SEC Phase	1.64	0.12
PEI Phase	2.65	0.98
DXE Phase	1.30	1.01
BDS Phase	3.14	3.52
Total	**8.72**	**5.64**



Source: Insyde software, Mobile Reference platform

- SEC and PEI Phase are highly optimized.
- 66% reduction in boot time.
- System still passes Microsoft WLK 1.4 tests

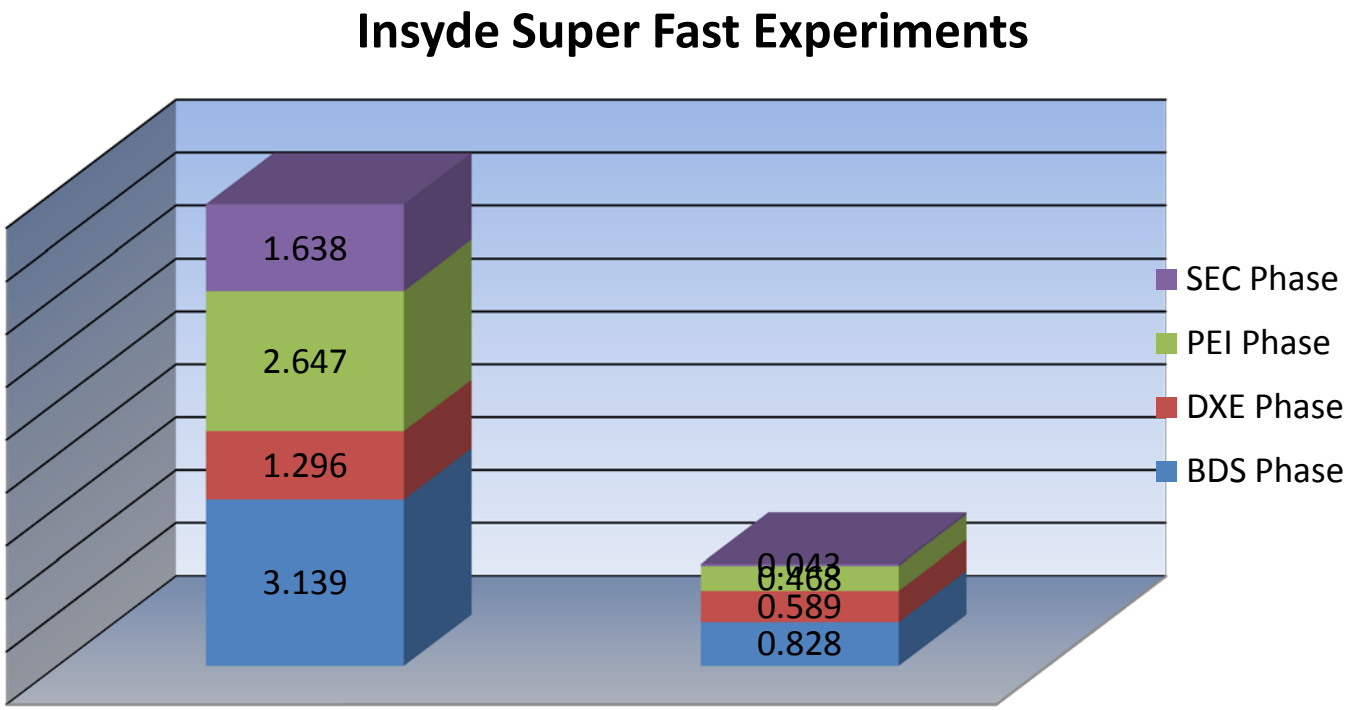
1 – InsydeH2O Calpella Tag 3.59.33.1039

Calpella is the codename for the mobile platform based on the Intel® 5 series-M chipset

Arrandale is the codename for a two core mobile processor used on the Intel® 5 series chipset based platforms codenamed Calpella.

“Break the rules” improvements

Task	Before (sec)	After (sec)
SEC Phase	1.64	0.04
PEI Phase	2.65	0.47
DXE Phase	1.30	0.59
BDS Phase	3.14	0.83
Total	**8.72**	**1.93**



Source: Insyde software, Mobile Reference platform

- Highly optimized for a <2 second boot.
- System does NOT pass Microsoft WLK 1.4 tests

Agenda

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

DEMO

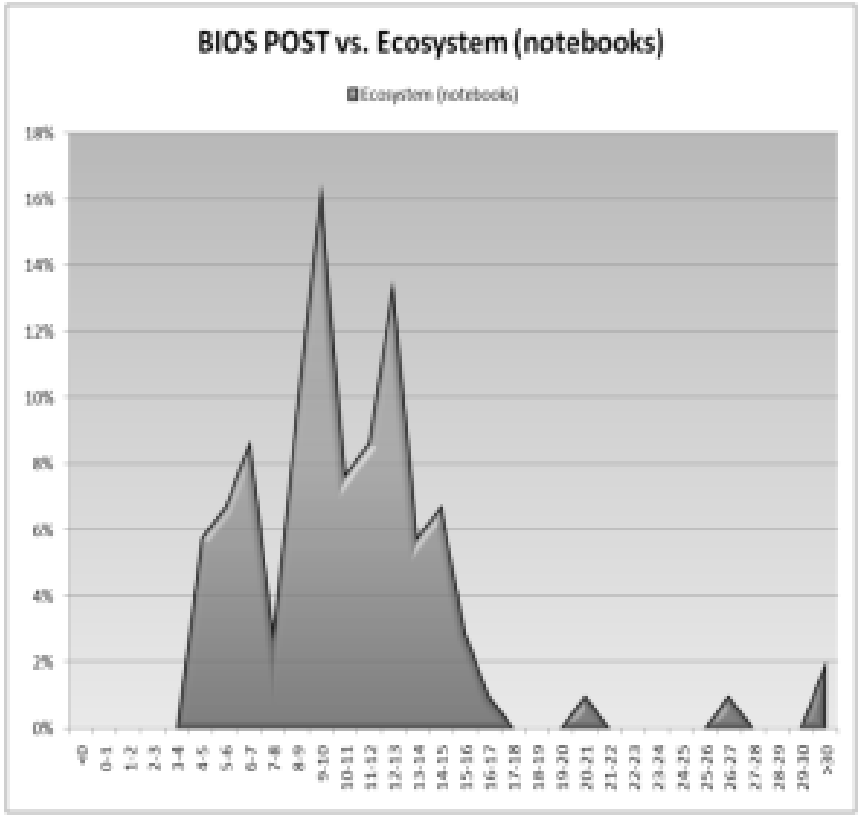
- Demo showing Windows® 7 booting **with** boot optimization on a notebook
- Windows Vista® on another notebook **without** the boot optimization

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

- 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 Vista SP1 on any HW, long POST times are more noticeable and undesirable for end users



"Source: Microsoft Windows OEM Engineering Services"

Microsoft

Agenda

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

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 high-end machines with Windows® 7
  - Verify that there are no race conditions or other compatibility problems
  - Verify both boot and hibernate use cases

Microsoft

Other Windows® 7 Considerations

- Memory Type Range Register (MTRR)
  - Ensure that MTRRs for each CPU is restored after S3 resume
  - If you don't, both firmware and OS resume code in HAL will run w/o caches enabled
  - In Windows® 7 because we always scan and validate the contents of the first 1Mb of physical memory when resuming from S3 as opposed to Vista where this scan does not occur by default
  - Adds ~400 milliseconds
  - Please note that this problem also will adversely impact the time it takes to synchronize the processor TSCs (new for Windows® 7) as this code depends on the processors caches being enabled.

Microsoft

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

Microsoft

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.

Microsoft

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.

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- Visit UEFI Booth #136 & Insyde SW #312
- 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
- Microsoft Boot Optimization White Paper: http://www.microsoft.com/whdc/system/platform/firmware/FirmwareEnhance_Win7.mspx.
- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress

IDF 2009 UEFI Sessions

EFI#	Company	Description	Time	RM	D
P001	Dell, HP, IBM, Intel, Microsoft	Using UEFI as the Foundation for Innovation	10:15	2005	T
S001	IBM, Intel	Intel Advanced Technology in the Enterprise: Best Security Practices	16:15	2001	W
S002	Dell, Intel, Insyde SW	Secure FW Lockdown through Standardized UEFI Management Protocols	17:15	2001	W
S003	Intel, AMI	Best Technical Methods for UEFI Development -Reducing Platform Boot Times -Firmware Debugging: UEFI and USB for platform forensics	11:10	2002	Th
S004	Microsoft, Insyde SW, Intel	UEFI Boot Time Opt. Under Microsoft Windows 7	13:40	2002	Th
S005	Phoenix, Intel	Transitioning the Plug-In Industry from Legacy to UEFI: Real World Cases	14:40	2002	Th
Q001	Intel, All	UEFI Q & A session	15:40	2002	Th

✓ DONE

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.
- Arrandale, Clarksfield, Calpella and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user
- 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, Core 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.
-

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.

Rev. 7/27/09