Using the Latest EFI Development Kit (EDK II) for UEFI Advanced Development and Innovation

Penny Gao - Senior Software Engineer, Intel
Ping Ping Han - Senior Software Engineer, IBM
Dong Wei - Distinguished Technologist, HP

EFIS001

Sponsors of Tomorrow. intel

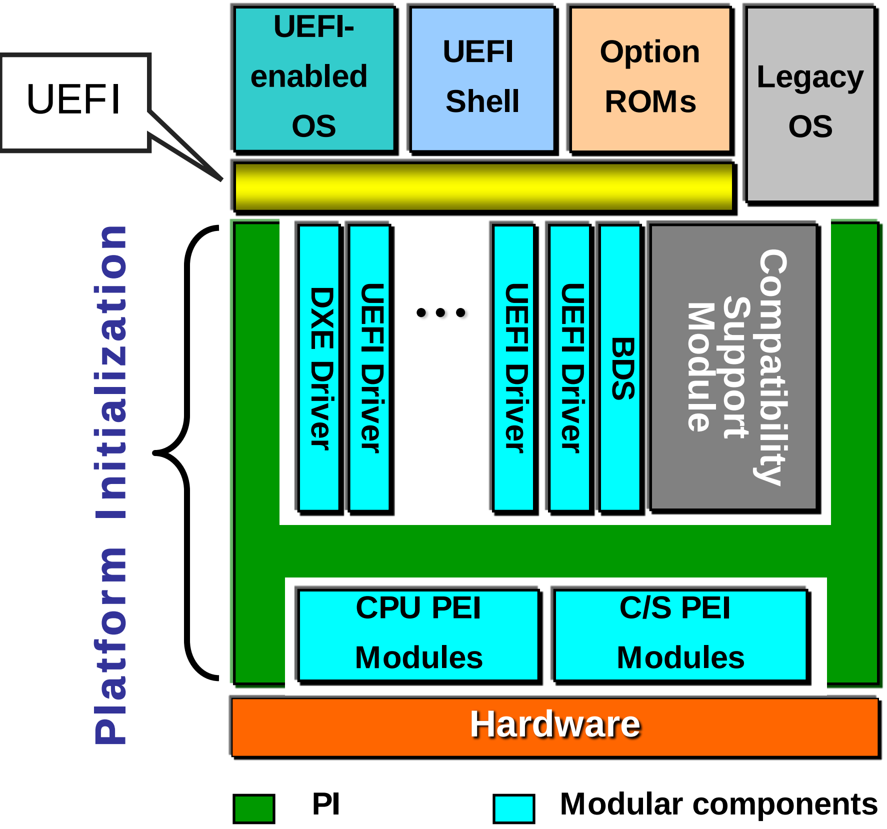
Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- EFI Developer Kit II (EDK II) Overview
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products using EDK II

Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- EFI Developer Kit II (EDK II) Overview
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products using EDK II

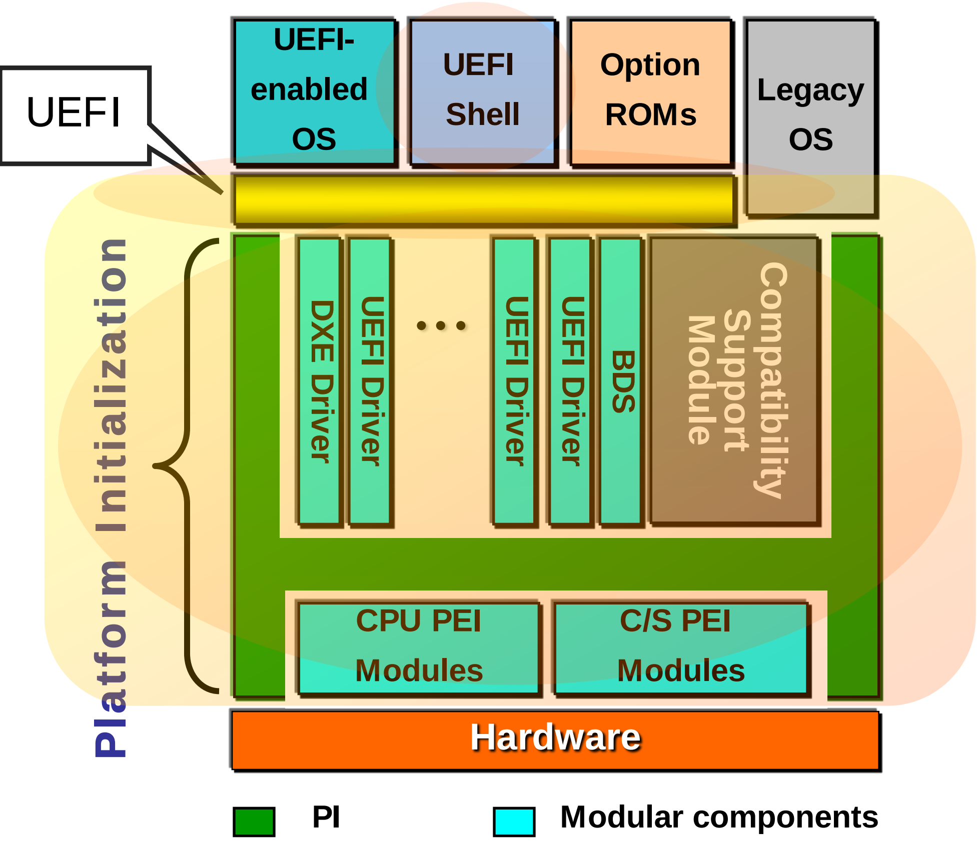
Standard Firmware Interfaces



- 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

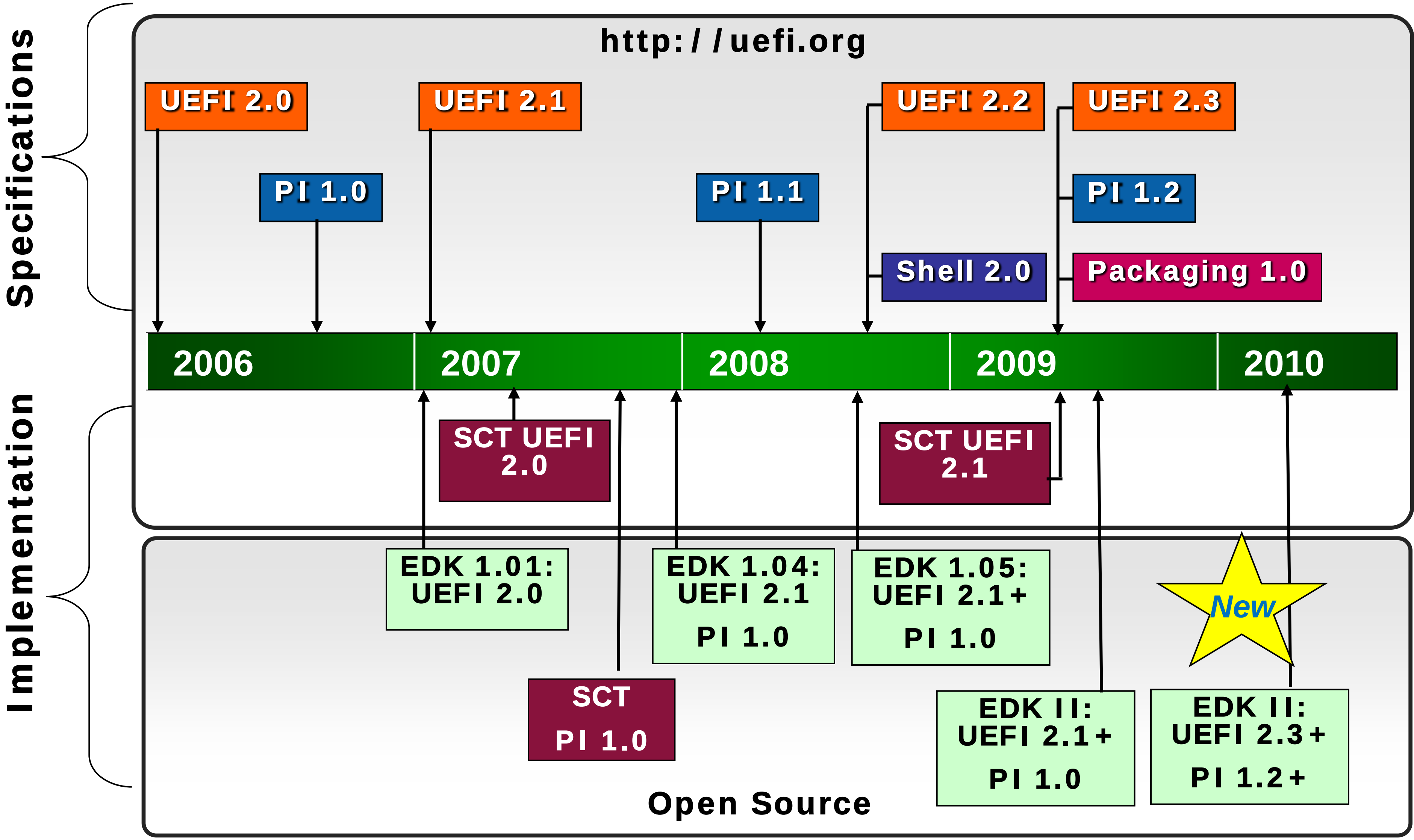
Latest UEFI Specifications



- *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

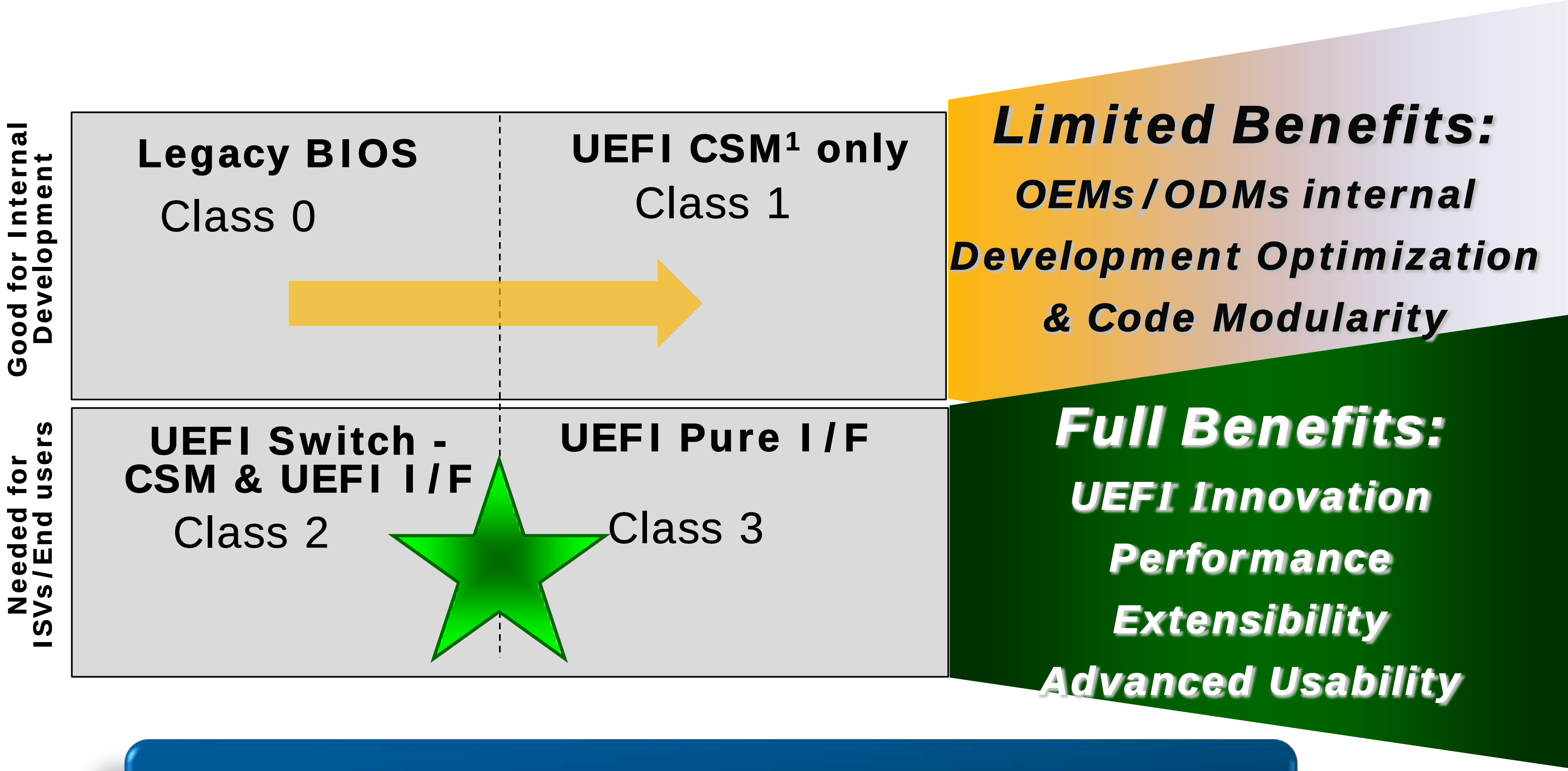


All products, dates, and programs are based on current expectations and subject to change without notice.

Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- EFI Developer Kit II (EDK II) Overview
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products using EDK II

Utilize UEFI Full Potential



Good for Internal Development

Needed for ISVs/End users

Legacy BIOS

Class 0

UEFI CSM[1] only

Class 1

UEFI Switch - CSM & UEFI I/F

Class 2

UEFI Pure I/F

Class 3

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

Easier to configure and deploy

- 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

Makes Computers more manageable

- Creates a common infrastructure for managing all machines
- Enable secure automated management – lower risks of "Rogue" servers or clients on the network

Network Scalable and Secure Firmware

- Enhanced networking APIs in the pre-boot network stack
- Richer network authentication (log-on)
- UEFI Certificate Authority for interoperable trust

Breaks through BIOS barriers

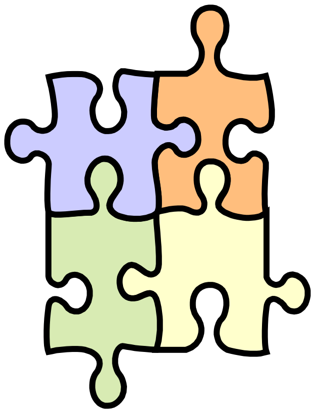
- Free from architectural limitation - scales technology across all platforms (Server, Desktop, Mobile, and Handheld)
- Access to disk range beyond 2TB – utilization of resources
- Option Rom Decongestion

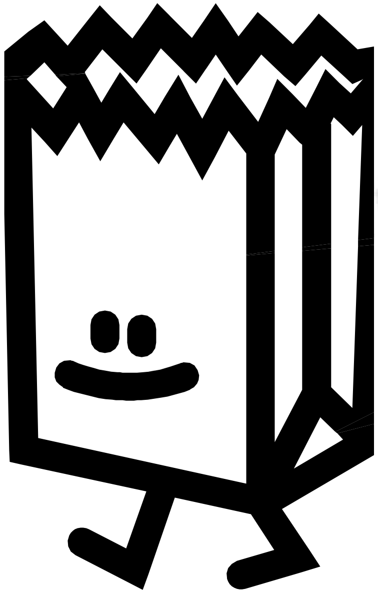
Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- EFI Developer Kit II (EDK II) Overview
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products using EDK II

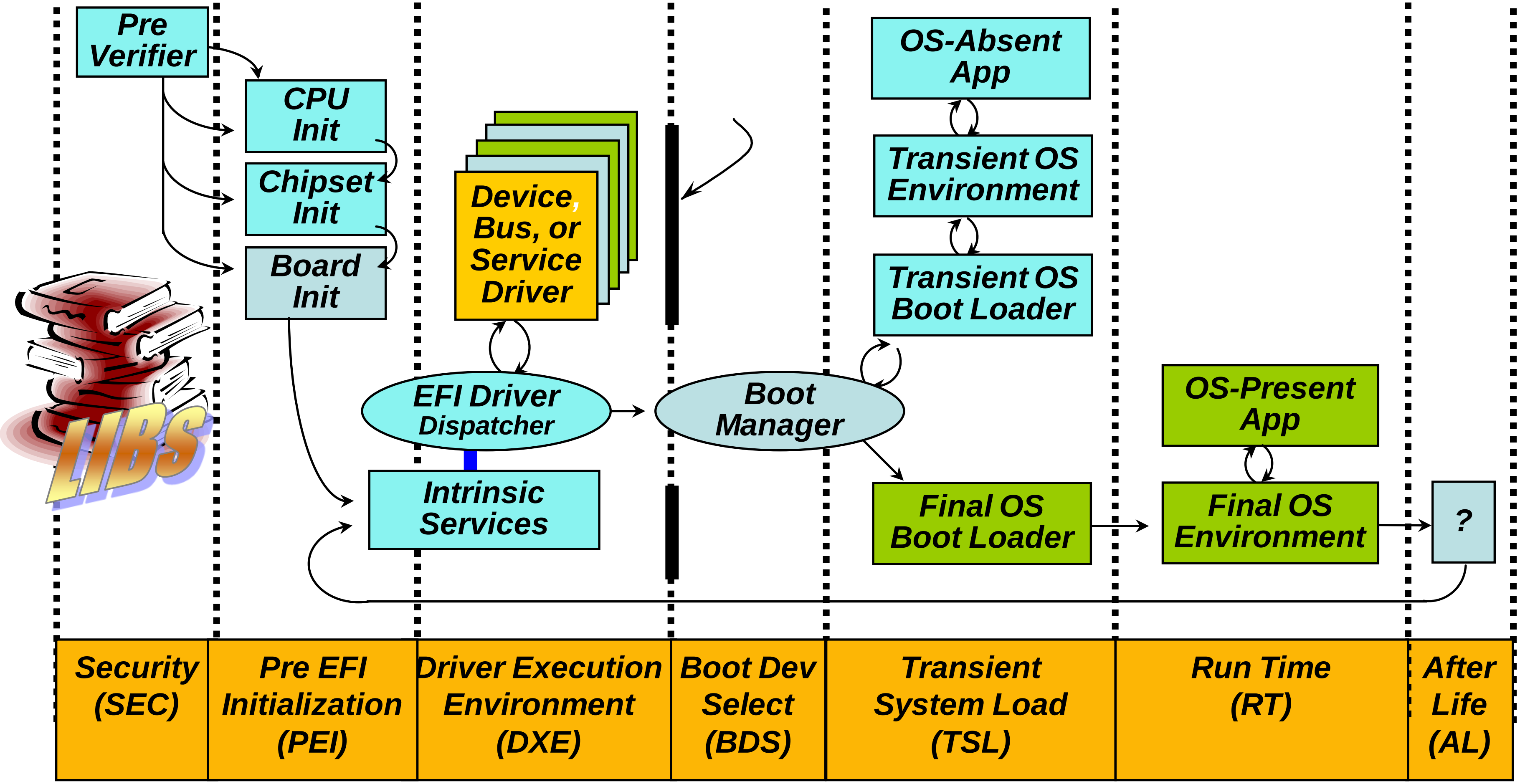
Package Philosophy

- As standards evolve there is a need to target your development on the set of standards you care about
- Solution: break the EDK II up into “packages” and enable customers to make their own packages.
- Only package together what is needed





Libraries - UEFI /PI Execution Phases



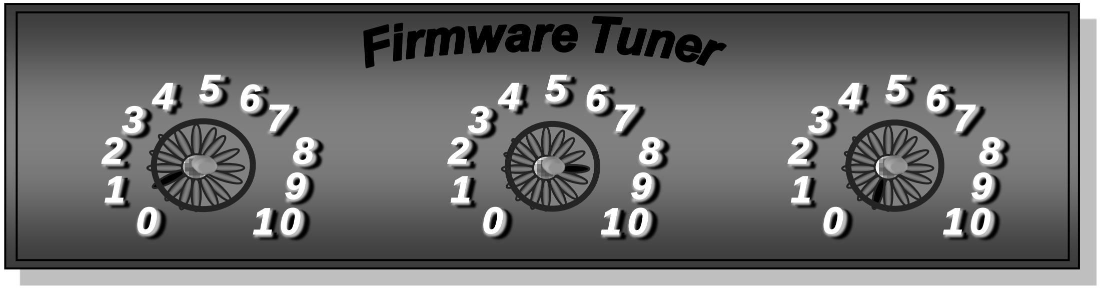
Power on → [. . Platform initialization . .] → [. . . . OS boot . . . .] → Shutdown

Same lib classes exist across multiple phases

Platform Configuration Database

Knobs to fine tune your firmware

- PCD entries are used for module “parameterization”.
- Benefits:
  - Reduce the need to edit source code
  - No searching for “magic” #define statements
  - Maximize module reuse across platforms
  - APIs for access to PCD entries
- PCDs can store platform information
  - Vital Product Data (VPD)
  - Serial Number, etc...
  - Setup options



Maximizes the re-use of modules
Minimize Source code editing

EDK II Benefits Package Distribution

- *UEFI Packaging 1.0 Specification*

Distribution Package File (ZIP, .dist)

Disttribution Description File (XML, .pkg)

Disttribution Content File (ZIP, .content)

Distribution Description File

```
<DistributionHeader ReadOnly" true" RePackage="false">
  <Name BaseName="NosuchChipset">
     NosuchChipset</Name>
  <GUID Version="1.2">AF0DDA2E-EA83-480b-B2CE-
     FC0BB2F894C2</GUID>
  <Vendor>NosuchCorporation</Vendor>
  <Date>2008-03-24T09:30:00</Date>
  <Copyright>Copyright©2008, NosuchCorporation.All
     rights reserved.</Copyright>
```

Description Content File

```
Workspace Directory
   BaseTools\
   Conf\
   NoSuchCorpPkg \
      Bus \
        Pci \
        PeerBusDxe \
        PciBusDxe \
        SuperDuperIODxe\
      Include \
        Common \
        GUID \
        • • •
   MdePkg \
   MdeModulePkg\
```

EDK II Implementation of UEFI makes everything just WORK!!!

Agenda

- UEFI Technical Specifications updates
- Using UEFI as an enabling foundation for platform innovation
- EFI Developer Kit II (EDK II) Overview
- Industry leaders discussing how UEFI is helping them innovate and differentiate their products using EDK II

IBM EDKII Era:
EDKII Innovation on System x Servers

Ping Ping Han

Senior Software Engineer

China System & Technology Lab, IBM

© 2010 IBM Corporation

Agenda

- IBM's Role in uEFI
- IBM EDK Based System x Servers
- Embracing EDKII
  - What value EDKII adds to development effort
  - What value EDKII adds to the customer & OEM
- IBM Value Add in EDKII
- IBM eX5 Launch on EDKII Based Products

© 2010 IBM Corporation

IBM’s Role in UEFI

- One of 11 uEFI forum promoters
- uEFI in System x Servers
  - Global Development (4+ time zones)
    - Raleigh
    - Austin
    - Kirkland
    - Shanghai/Taipei
  - 2007 kick off
  - 2009 ship the first product based on EDK
  - 2010 ship EDKII based System x servers

© 2010 IBM Corporation

Agenda

- IBM’s Role in uEFI
- IBM EDK Based System x Servers
- Embracing EDKII
  - What value EDKII adds to development effort
  - What value EDKII adds to the customer & OEM
- IBM Value Add in EDKII
- IBM eX5 Launch on EDKII Based Products

© 2010 IBM Corporation

EDK Based System x Servers

- Comprehensive transition of the System x portfolio to UEFI based firmware
- UEFI 2.1 PI 1.0 specification compliant

Blade

- HS22
- HS22V

Rack-mount

- x3650 M3
- x3550 M3
- X3250 M3

Tower

- x3500 M3
- x3400 M3
- x3200 M3

Large-scale

- dx360 M3

© 2010 IBM Corporation

Agenda

- IBM’s Role in uEFI
- IBM EDK Based System x Servers
- Embracing EDKII
  - What value EDKII adds to development effort
  - What value EDKII adds to the customer & OEM
- IBM Value Add in EDKII
- IBM eX5 Launch on EDKII Based Products

© 2010 IBM Corporation

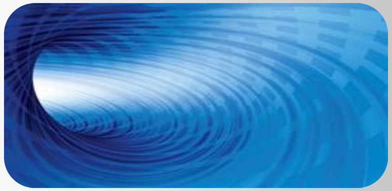
EDKII benefits to development effort

Package resource

- Package can come from different providers, such as TianoCore, IHV etc

Integration effort

- Reduce integration effort with package based release
  - Dramatically lower integration time for Intel code drops (Intel code is mostly touchless in EDKII)



Developer efficiency

- Improve developer efficiency
  - Much better build time
  - Better/more complete code documentation
  - Strong/Explicit package structure to support isolation and clean Core/Platform model
  - New features such as PCD, Library class speed up the development

© 2010 IBM Corporation

EDKII benefits to customers & OEMs

More standardized, more features and consistent look & Feel

– EDKII core code more strictly follows the UEFI and PI standards.

– New features will be more likely to be integrated to the EDKII products such as IPv6 etc

– More consistent look & feel and operation since more code is shared

Easy for OEM vendor to re-configuration

– OEM vendor can configure the OEM firmware according to their requirement

© 2010 IBM Corporation

Agenda

- IBM’s Role in uEFI
- IBM EDK Based System x Servers
- Embracing EDKII
  - What value EDKII adds to development effort
  - What value EDKII adds to the customer & OEM
- IBM Value Add in EDKII
- IBM eX5 Launch on EDKII Based Products

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

Standardized Pre-boot Security

- TPM & Core Root of Trust for Measurement support (CRTM)
- Secure Update methods

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

Standardized Pre-boot Security

- TPM & Core Root of Trust for Measurement support (CRTM)
- Secure Update methods

Advanced memory RAS technology

- Memory Predictive Fault Analysis Alerts
- DIMM Isolation

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

Standardized Pre-boot Security

- TPM & Core Root of Trust for Measurement support (CRTM)
- Secure Update methods

Advanced memory RAS technology

- Memory Predictive Fault Analysis Alerts
- DIMM Isolation

Green Energy: Active Energy Manager (AEM)

- Power metering, power capping, power saving

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

Standardized Pre-boot Security

- TPM & Core Root of Trust for Measurement support (CRTM)
- Secure Update methods

Advanced memory RAS technology

- Memory Predictive Fault Analysis Alerts
- DIMM Isolation

Green Energy: Active Energy Manager (AEM)

- Power metering, power capping, power saving

Out-of-band configuration and update capabilities

- Configure and update uEFI firmware via out-of-band tools such as ASU, iFlash etc

© 2010 IBM Corporation

IBM Value Add in EDKII

Key features beyond the basic requirements of uEFI firmware

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)

Standardized Pre-boot Security

- TPM & Core Root of Trust for Measurement support (CRTM)
- Secure Update methods

Advanced memory RAS technology

- Memory Predictive Fault Analysis Alerts
- DIMM Isolation

Green Energy: Active Energy Manager (AEM)

- Power metering, power capping, power saving

Out-of-band configuration and update capabilities

- Configure and update uEFI firmware via out-of-band tools such as ASU, iFlash etc

Multi-node support

- Intel® Xeon® 7500, memory etc

© 2010 IBM Corporation

Agenda

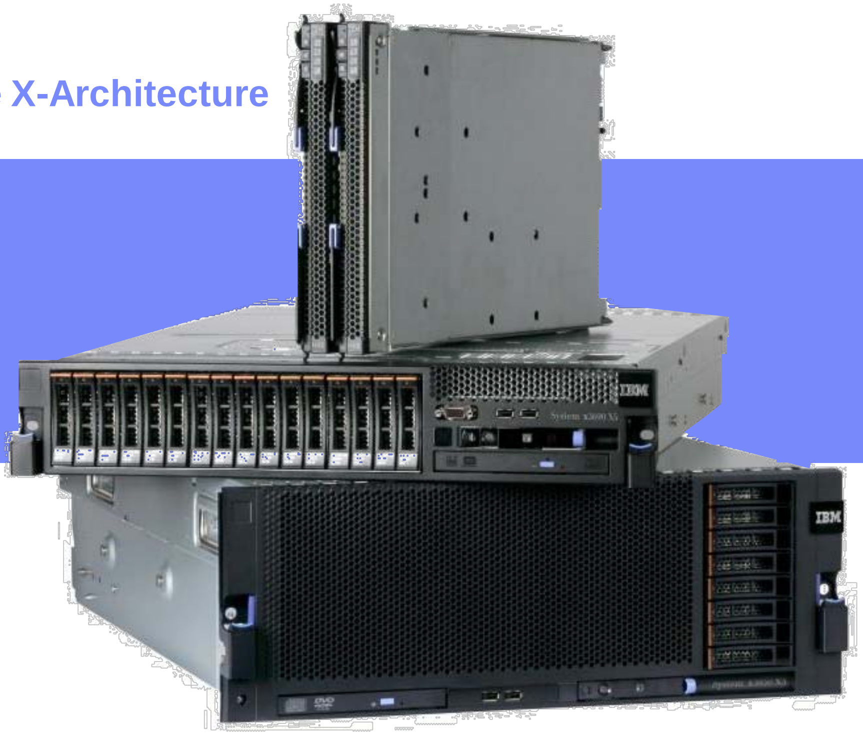
- IBM’s Role in uEFI
- IBM EDK Based System x Servers
- Embracing EDKII
  - What value EDKII adds to development effort
  - What value EDKII adds to the customer & OEM
- IBM Value Add in EDKII
- IBM eX5 Launch on EDKII Based Products

© 2010 IBM Corporation

Maximize Memory
Minimize Cost
Simplify Deployment

The fifth generation technologies of IBM Enterprise X-Architecture

The broadest portfolio of systems optimized for your most demanding workloads



eX5 Systems represent a broad portfolio including racks & blades

BladeCenter HX5 Extends the value of Enterprise X-Architecture to BladeCenter

System x3850 X5 Enhances the current generation with more capability than ever

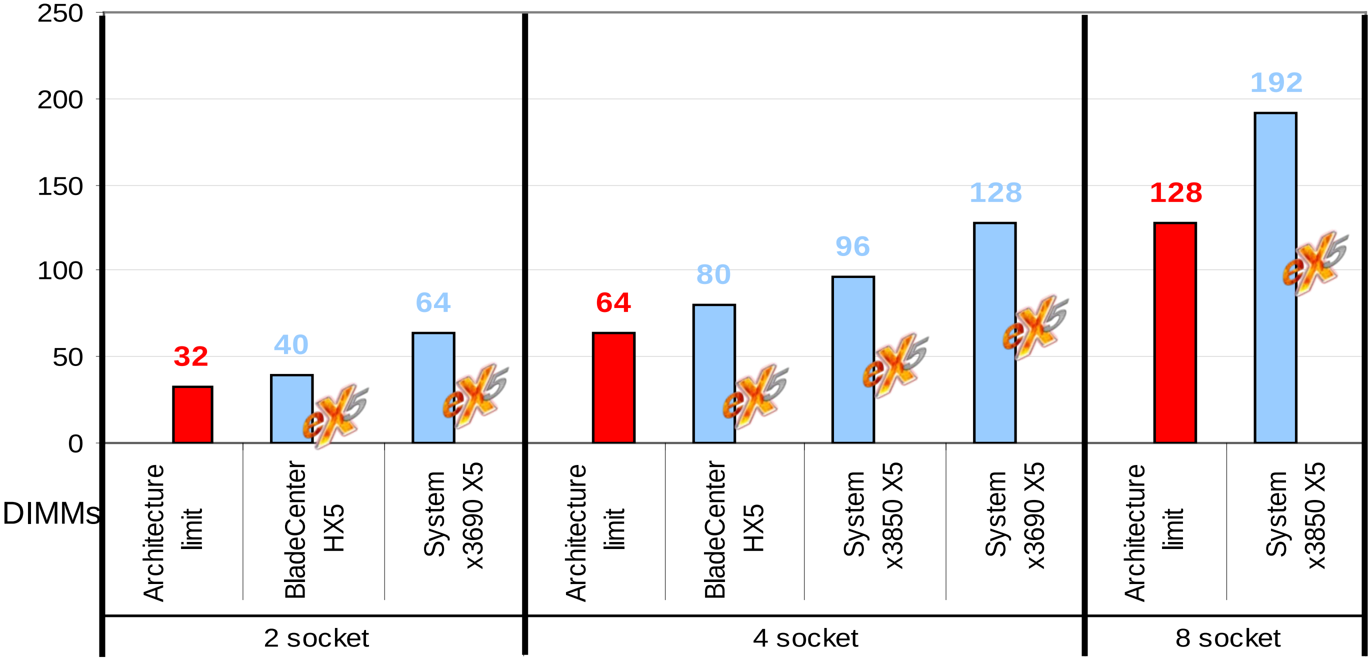
System x3690 X5 A new design offering best density for enterprise computing

© 2010 IBM Corporation

MAX5: Maximizes memory capacity above x86 limit

MAX5 for eX5 racks and blades enables more, larger, faster databases and virtualization workloads

MAX5 enables up to 192 DIMMs or 3 TB of system memory



© 2010 IBM Corporation

EDK II Transition

On HP Integrity Servers

Dong Wei – HP Distinguished Technologist
April 14, 2010

© 2010 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

Reproduced with Permission

Global Companies Depend on Itanium® for Their Mission Critical IT Infrastructure

Efficient Energy Delivery

Nearly all G100 Energy Companies

Efficient Automotive Manufacturing

75% G100 Automobile Manufacturers

More

Efficient Manufacturing

75% G100 Electronic Manufacturing Companies

Better Healthcare Delivery

75% G100 Health Care Companies

Delivering New Telecom Services

Nearly all G100 Telecom Providers

More than 80 of top Global 100 companies running Itanium®

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

The Only Common CPU Architecture Across x86 and Unix

Common Platform Ingredients:

Intel® QuickPath and Scalable Memory Interconnects

Intel® 7500 Scalable Memory Buffer and DDR3

Intel® 7500 Chipset

Intel® Itanium® 9300

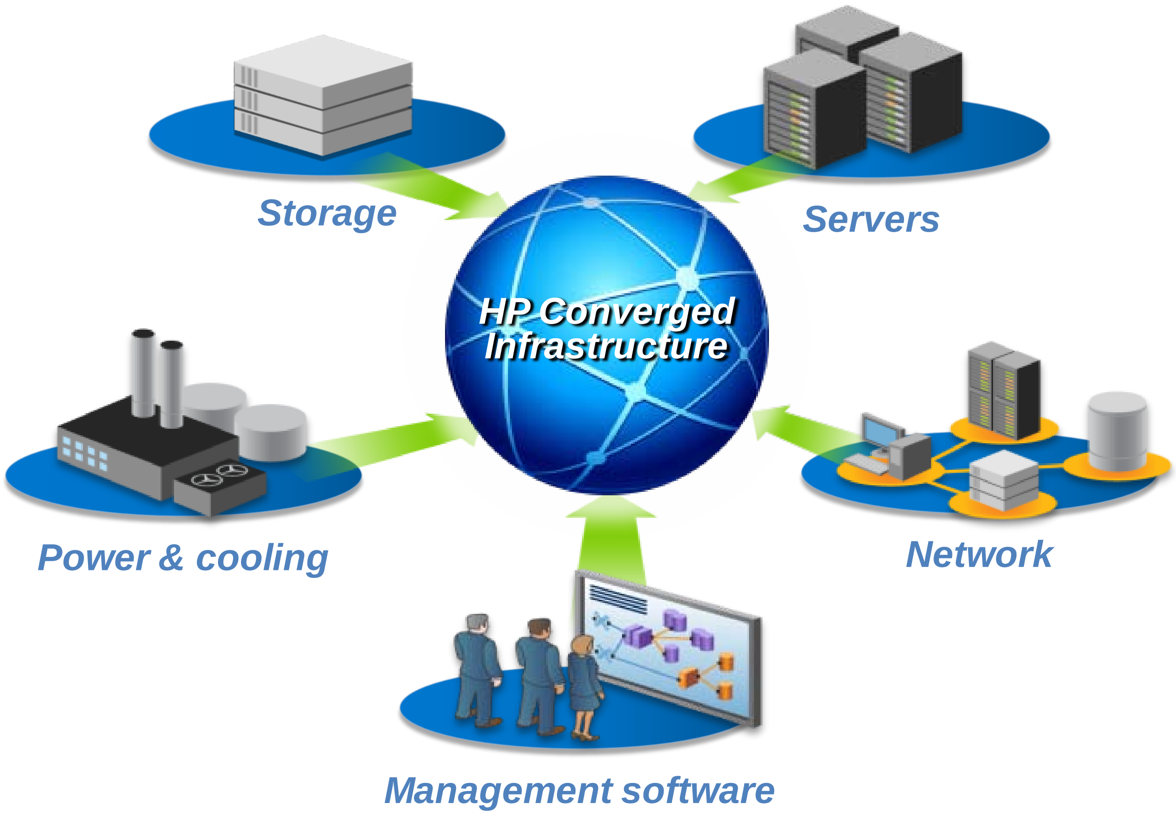
Intel® Xeon® 7500

Mission Critical Performance, Shared Infrastructure

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

HP Integrity Servers

The Mission Critical Backbone of a Converged Infrastructure



Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

HP Integrity Servers based on Intel's Itanium® 9300-series Processors

Delivers:

- Greater virtualization flexibility
- Simplicity through standardization
- Greener IT
- No compromise on RAS
- Dynamic scalability

Three significantly different platforms

- Rack-mount servers
- BladeSystems
- Superdome

Processor and chipsets

- Intel® Itanium® 9300-series processors
- Intel® E7500 Scalable Memory Buffer
- Intel® E7500 IOH, and ICH10
- HP-designed chipset for scalability

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

Transition to EDK II

- Integrity servers leading the way in HP in the transition
- All three platforms transitioned to EDK II
  - Have a single source tree
  - Benefited from the superior package-oriented architecture
    - Ability for reuse and single module/solution owners. Once a bug is fixed, every platform sees the benefit.
  - The EDK Compatibility Package works very well
    - Reuses existing silicon modules
    - Build the UEFI shell

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

Lessons Learned

- Challenges
  - The continuous reference source tree updates from Intel
    - To keep up, we had to perform multiple large-scale source tree merges once every 2-3 months on average
    - Opportunities for improvements
  - A shared environment
    - some of this can be reduced by using the EDK II package solution to create platform specific modules when needed.

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

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 – use the EDK II Implementation
- Make use of the rich UEFI community resources

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications sites www.uefi.org, www.intel.com/technology/efi
  - EDK II Open Source Implementation: www.tianocore.org

- 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, 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 © 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