UEFI Advancements for Independent Hardware Vendors

Mike Rothman – Intel Corporation
Anand Joshi – Dell Inc.
Uma Parepalli – LSI Corporation
Dick Wilkins – Phoenix Corporation

EFIS002

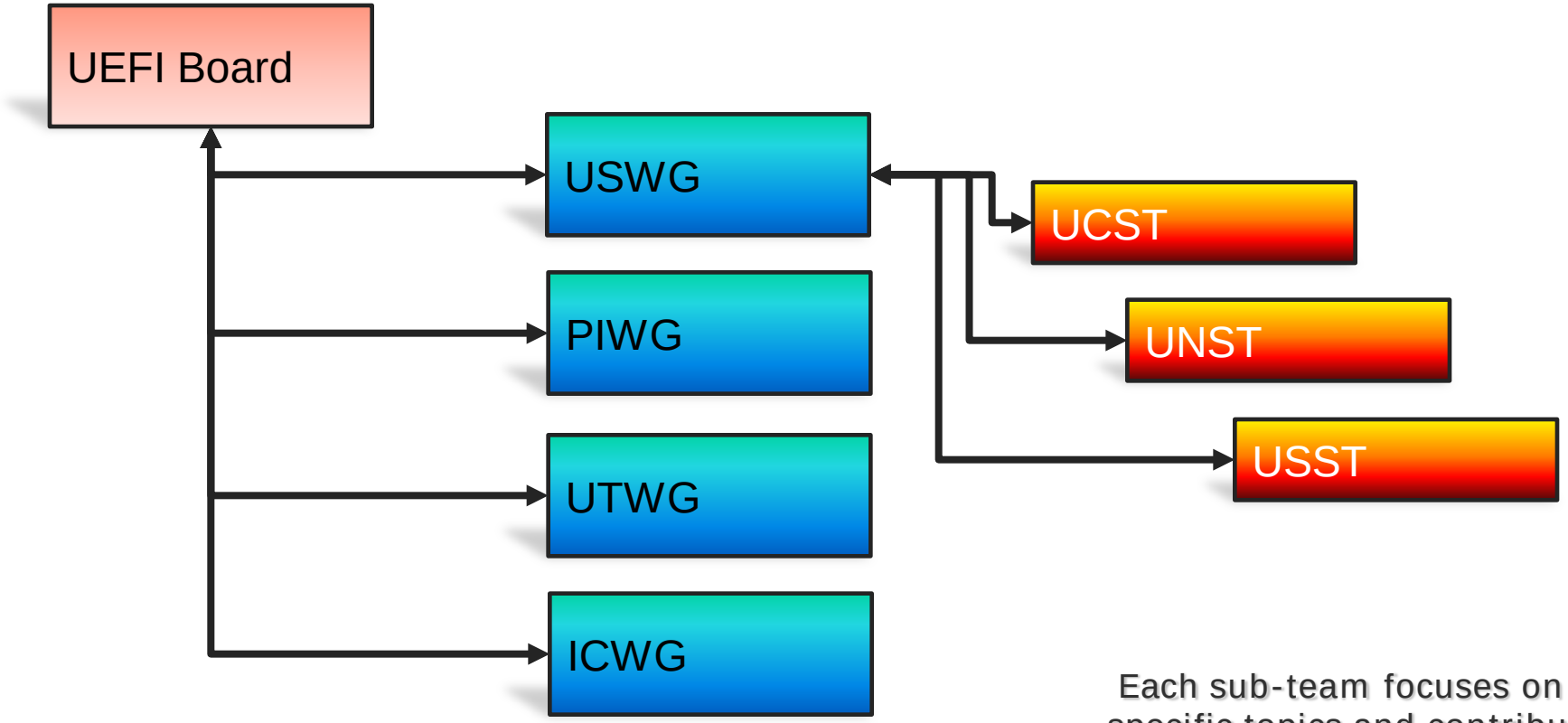
Agenda

- Review of IHV applicable UEFI features
- UEFI Benefits to IHVs
- Recommendations from Dell
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

Agenda

- Review of IHV applicable UEFI features
- UEFI Benefits to IHVs
- Recommendations from Dell
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

The UEFI Forum



Publications/Decisions ratified by the board

Each work group approves/delivers different content to the public.

Each sub-team focuses on specific topics and contributes material to the work group.

BIOS Standards emerge from the UEFI work groups

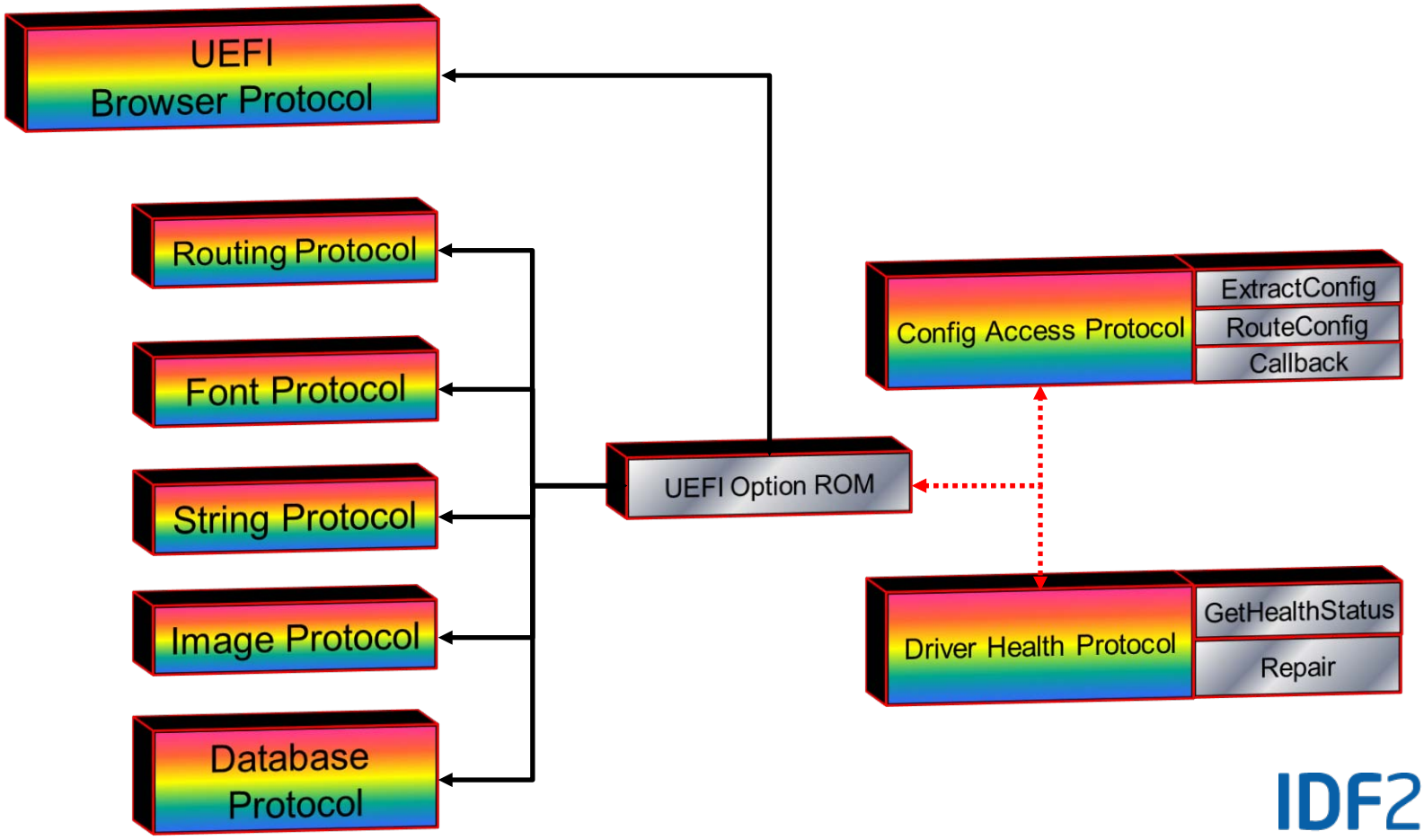
UEFI Features – Configuration Infrastructure

- Forms-based model for setup question descriptions
  - Must meet BIOS requirements
    - Scalable UI display support (Server Front Panel to local high resolution monitor).
    - Small encoding size
  - Encoding that is Self Describing
  - Can support scripting
  - Extensible syntax
- Exact look and feel defined by the browser and not defined in UEFI.
  - Developer/OEM/IHV defines questions to ask and what strings to display
  - Browser determines “how” to display the questions HII

UEFI provides a simple yet powerful method to describe configuration data

Configuration Infrastructure Protocol Overview

- IHVs should use these protocol interfaces for the configuration infrastructure



UEFI Features – Configuration Infrastructure

- With forms, we introduce localization

Spanish

US English

French

String ID #4	String Representation	H	E	L	L	O		W	O	R	L	D	
	Unicode Encoding	0x0048	0x0045	0x004C	0x004C	0x004F	0x0020	0x0057	0x004F	0x0052	0x004C	0x0044	0x0000

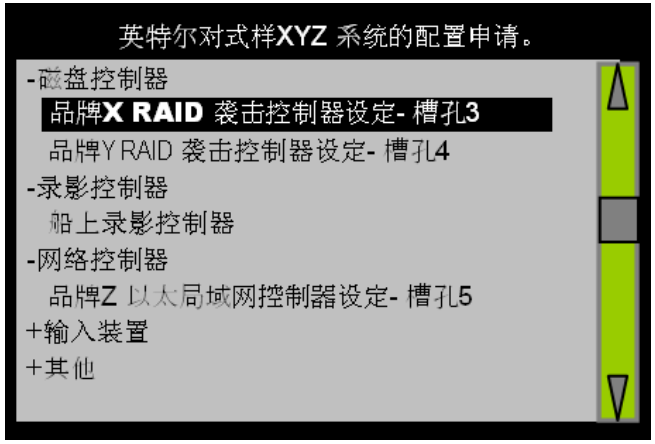
String ID #4	String Representation	H	O	L	A		M	U	N	D	O	
	Unicode Encoding	0x0048	0x004F	0x004C	0x0041	0x0020	0x004D	0x0055	0x004E	0x0044	0x004F	0x0000

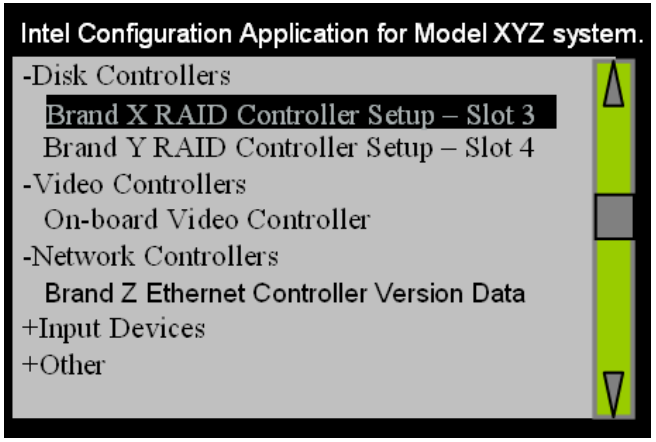
String ID #4	String Representation	你	好	世	界	
	Unicode Encoding	0x4F60	0x597D	0x4E16	0x754C	0x0000

Both input and output localization is supported

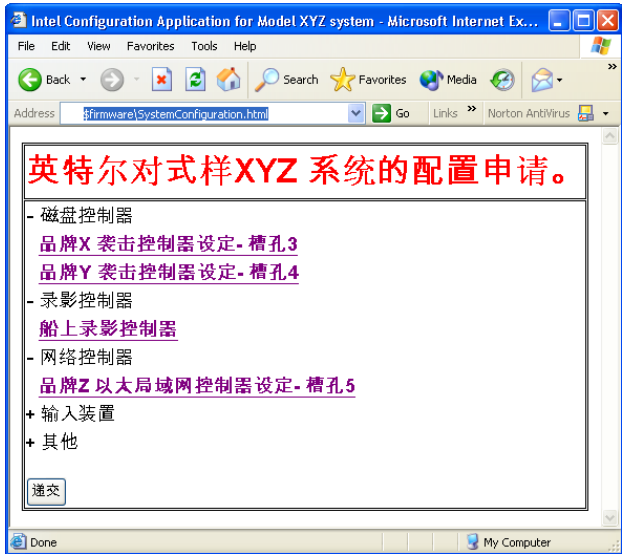
UEFI Features – Configuration Infrastructure

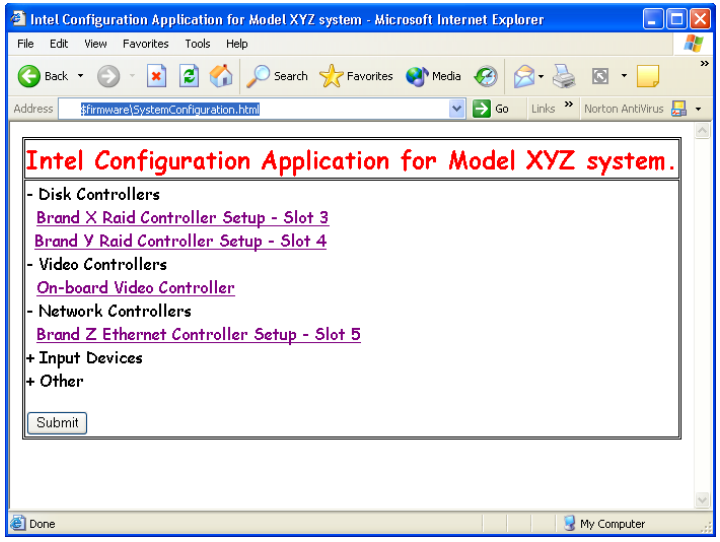
- Rudimentary Mock-up of Interfaces





Pre-O/S

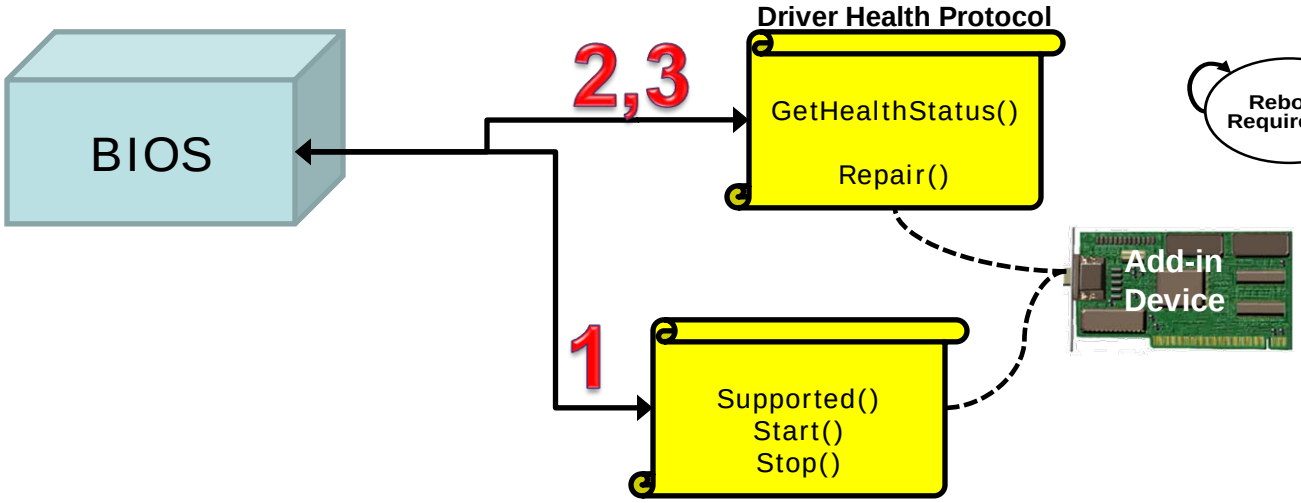


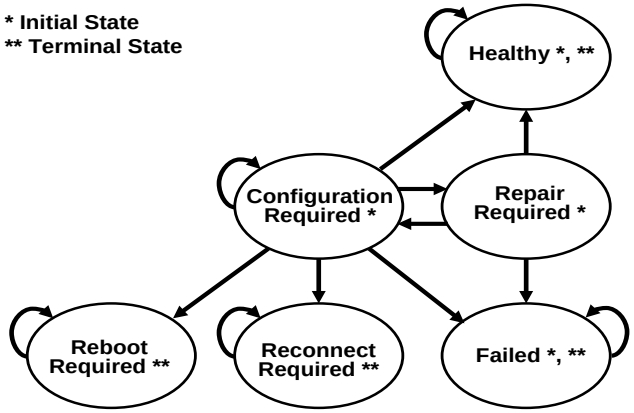


Runtime

UEFI Features – Driver Health

- Driver Health Protocol





1) UEFI BIOS attempts to initialize a device with an option ROM
   a) Device runs into an issue which might be recoverable
2) UEFI BIOS checks on the health of the device
   a) Device may return some forms-based data references to the BIOS so it can optionally communicate with the user. It also returns status regarding the health (see state diagram in upper right).
3) UEFI BIOS can optionally interact with the user to notify them of the message the device wanted to communicate, and if the driver health indicated that repair was required, the BIOS can automatically call the option ROM's repair facility.

Option ROM can advertise health status

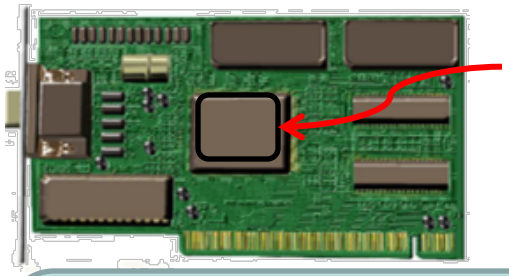
Agenda

- Review of IHV applicable UEFI features
- **UEFI Benefits to IHVs**
- Recommendations from Dell
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

UEFI Benefits to IHV – Remove some burdens

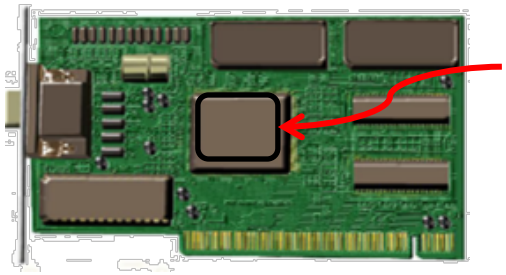
- Do not need to carry their own UI infrastructure
  - Less code/logic to support
  - By centralizing any key polling delays, speeds up platform booting.

Legacy Environment



1) Display Text/Logo
2) Poll for keystrokes (delaying boot)
   a) Present UI infrastructure
   b) Handle UI responses
3) Initialize Hardware

UEFI Environment



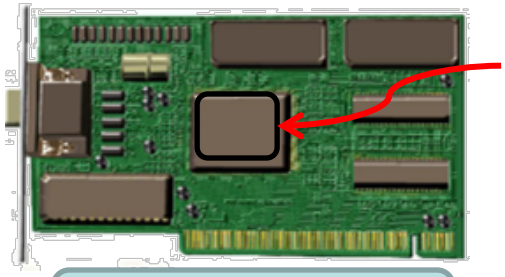
1) Register Content with platform
2) When called, initialize Hardware

Minimize IHV burden with UEFI

UEFI Benefits to IHV – Expand Configurability

- EBC (EFI Byte Code) allows a single image option ROM to operate on multiple CPU environments
- Maximal compatibility while minimizing binary size impact

Legacy Environment

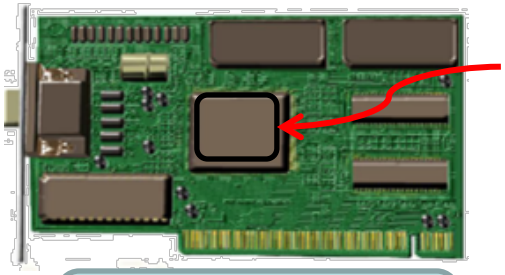


Binary Image for CPU type x

Binary Image for CPU type y

Binary Image for CPU type z

UEFI Environment

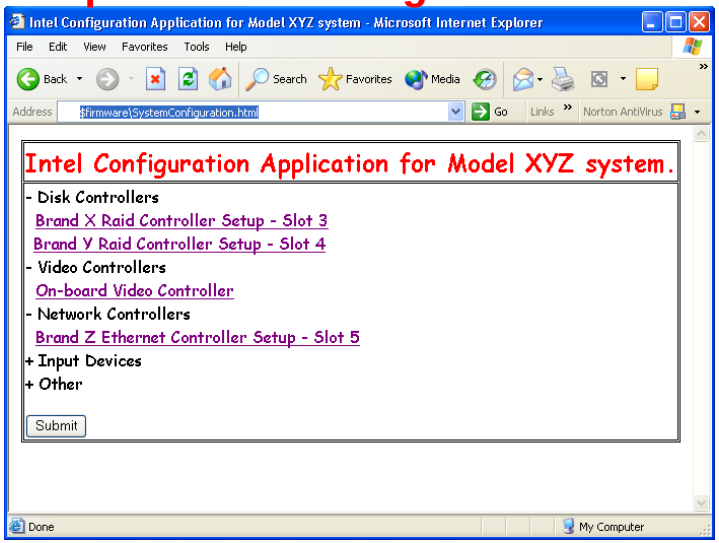


EBC Image for all CPU types running on UEFI

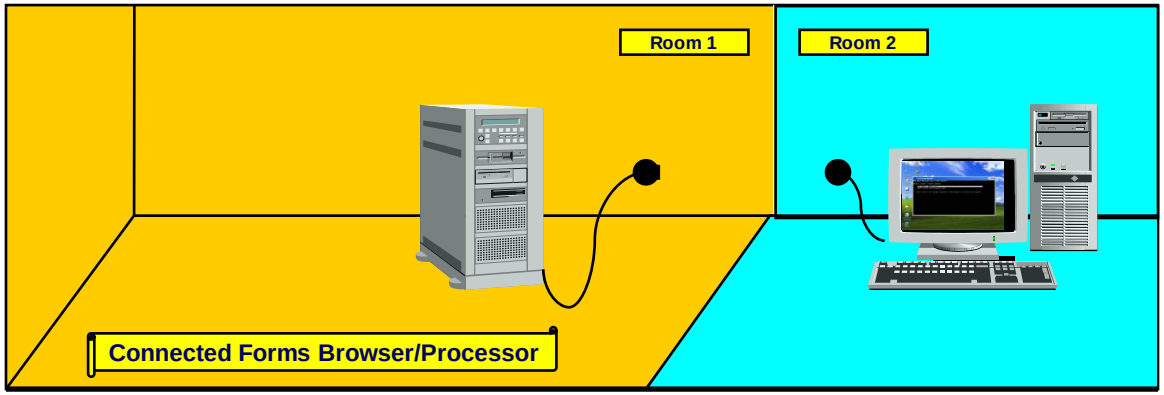
UEFI Benefits to IHV – Expand Configurability

- No longer a black-box
  - Can describe their payload and interact with platform in standard fashions
  - Expose content so that it can seamlessly be integrated in platform solutions.

Seamlessly integrate device data into the platform's configuration menu



Configure device(s) remotely



UEFI expands configurability of devices

Agenda

- Review of IHV applicable UEFI features
- UEFI Benefits to IHVs
- **Recommendations from Dell**
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

Why UEFI?

- Abstraction for the Operation System
  - Well defined API/interface between platform firmware
- Abstraction for devices and related code
  - Well defined driver model
  - Protocol based abstraction for range of underlying hardware devices
- Scalable environment
  - Protocol definition for contemporary platforms
  - Active standards body

Why UEFI?

- Rich Pre-Boot environment
  - Boot services and protocols through UEFI driver (device / service)
  - File system capabilities
  - Provide enhanced platform capabilities
    - firmware update, platform configuration, diagnostics and deployment services
- Breaking Boundaries
  - Support of 2.2 >TB boot disk

Dell sees huge value in UEFI and all Dell PowerEdge servers support UEFI

UEFI Device Driver

- Analogues to legacy option ROM
- Manages the controller
- All PCIe controllers or adapters must provide support for both Option ROM and UEFI driver
- Expansion Option ROM contains
  - Legacy
  - UEFI drivers
    - Processor Native X64 (preferred) and/or EBC
- Provides support for the primary feature of the Adaptor
  - Storage – Block IO protocol
  - Network – UNDI protocol

Protocols: To implement or not to implement that is the question

EFI_GRAPHICS_OUTPUT_PROTOCOL
EFI_BUS_SPECIFIC_DRIVER_OVERRIDE_PROTOCOL.
EFI_SIMPLE_TEXT_OUTPUT_PROTOCOL
EFI_DRIVER_HEALTH_PROTOCOL
EFI_DRIVER_DIAGNOSTICS2_PROTOCOL
EFI_BLOCK_IO_PROTOCOL
EFI_ATA_PASS_THRU_PROTOCOL
EFI_SIMPLE_TEXT_OUTPUT_PROTOCOL
EFI_COMPONENT_NAME2_PROTOCOL.
EFI_DRIVER_FAMILY_OVERRIDE_PROTOCOL
EFI_GRAPHICS_OUTPUT_PROTOCOL,
EFI_NETWORK_INTERFACE_IDENTIFIER_PROTOCOL,
EFI_DRIVER_BINDING_PROTOCOL
EFI_BLOCK_IO_PROTOCOL
OCOL

So many!!

Protocols: To implement or not to implement that is the question

- What is required depends of the type of the functionality that you offer
  - Device Driver?
    - Must support EFI_DRIVER_BINDING_PROTOCOL, EFI_COMPONENT_NAME2_PROTOCOL
  - Support disk devices?
    - EFI_BLOCK_IO_PROTOCOL is must
  - Section 2.6 of UEFI spec spells most it
  - Still there are lots of optional
    - Optional per spec
    - But required by the platform vendors

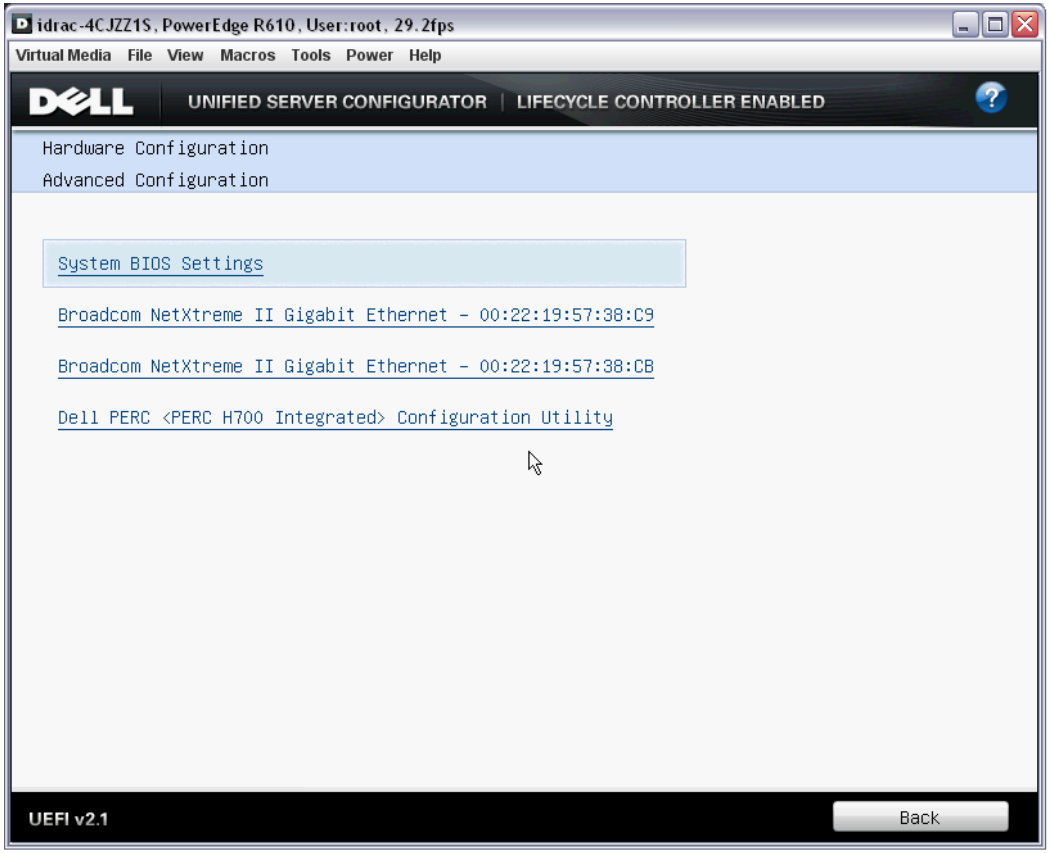
Protocols: To implement or not to implement that is the question

- Optional per spec…
- But required by Dell…

Many of Dell's value adds make use of the option components in the spec

Configuration: based on Human Interface Infrastructure (HII)

- Single window for all of the platform configuration
- Avoid multiple hotkeys
- Localization support
- Unified look and feel
- If driver supports any configuration, must be implemented using HII



Additional considerations for HII

- Localization support
- Dell expects support for US, fr-FR, de-DE, es-ES, ja-JP, zh-Hans
- EFI_COMPONENT_NAME2_PROTOCOL supports the languages specified
-
- Provide EFI_HII_DEFAULT_CLASS_STANDARD for all configurable items which can be set to default

- Limit call backs that dynamically modifies IFR.
- Instead, opcodes like grayoutif and suppressif can be used to dynamically change fields from read-only to read/write or dynamically suppress/un-suppress fields

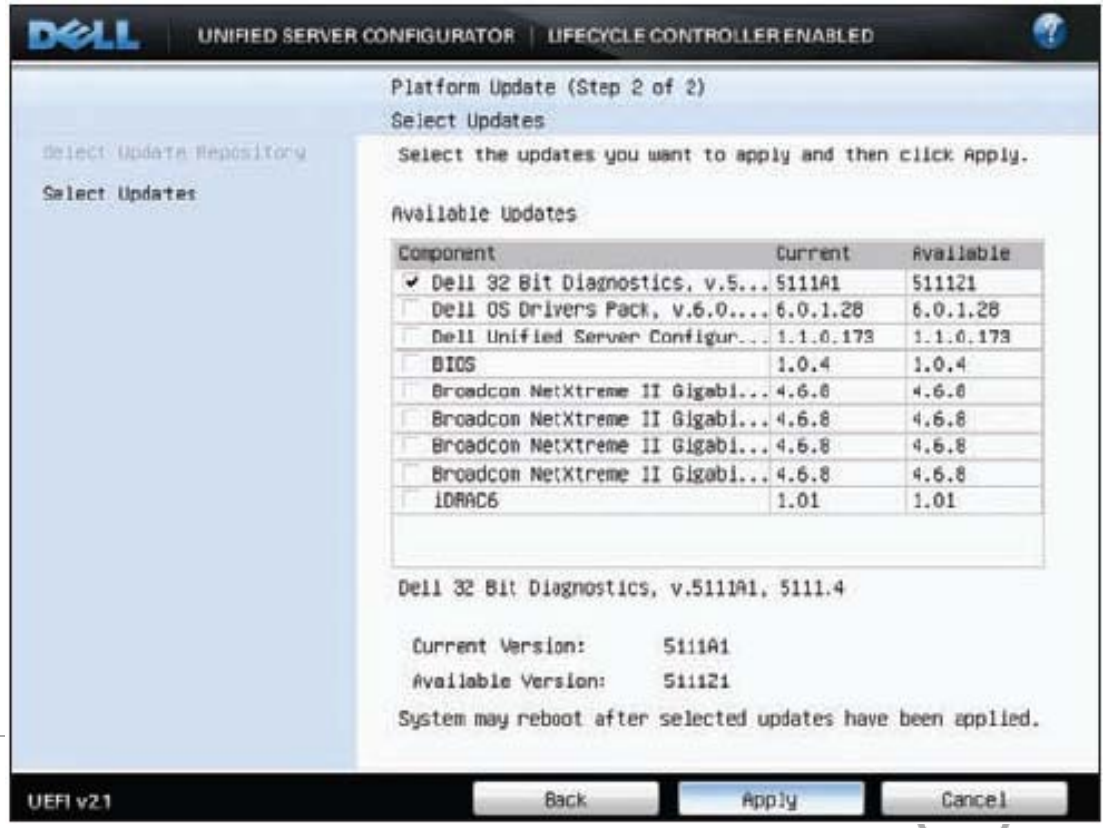
- Provide a title in the HII formset and form

Additional considerations for HII

- Set EFI_IFR_FLAG_RESET_REQUIRED for items that require a reboot to take effect. Do not use system reset in routeconfig or callbacks
- HII configuration drivers must implement EFI_IFR_FORM_SET_OP and set one of the ClassGuid[] to EFI_HII_PLATFORM_SETUP_FORMSET_GUID to indicate that the HII formset published by this driver is used for platform configuration.
- Consider Configuration Mapping Support using UEFI_CONFIG_LANG "UEFI-X". Please contact your OEM partner for additional information.
- **Any settings changes made via HII must take effect when booting in UEFI or in legacy BIOS mode**

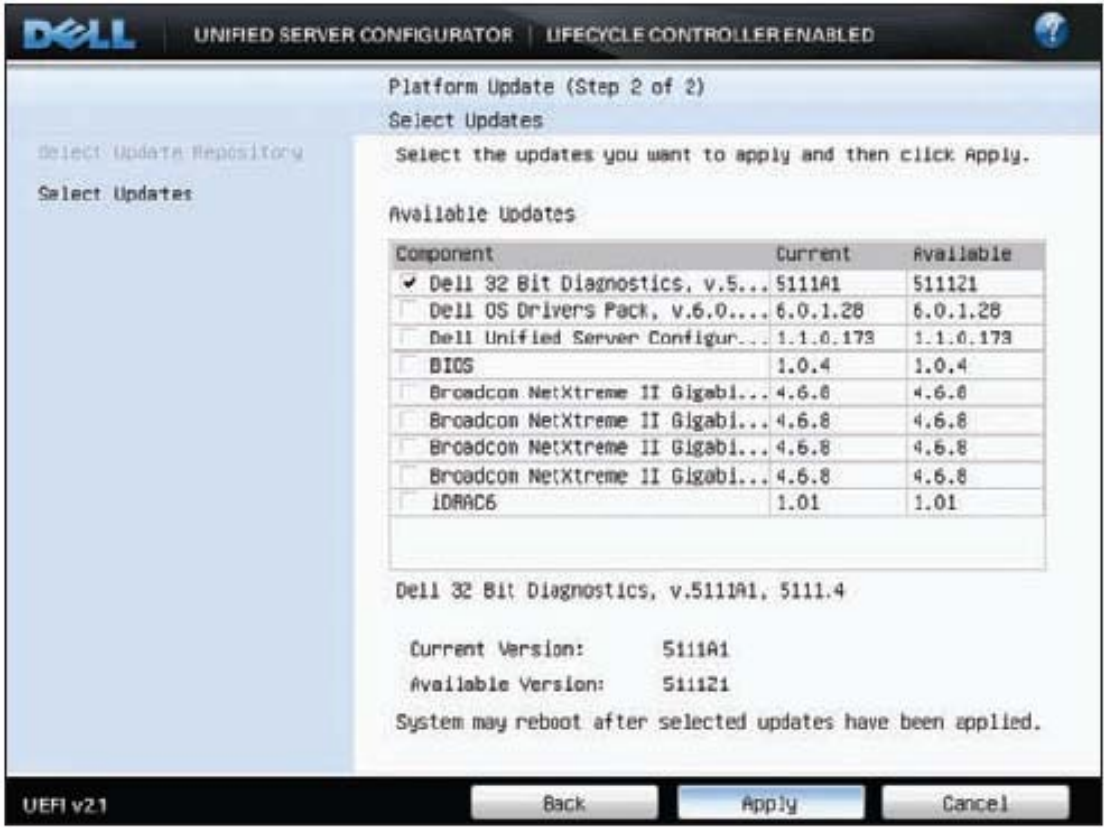
Updatable firmware:
EFI_FIRMWARE_MANAGEMENT_PROTOCOL (FMP)

- All adaptor firmware has some way to Manage firmware (Get firmware version, Update the image etc).
- Proprietary ways to common set of functions are not efficient
- FMP abstracts only the external interface not the actual update logic
- FMP makes managing firmware easy through providing a common UI for all firmware updates
- **FMP is required for Dell PowerEdge Servers**



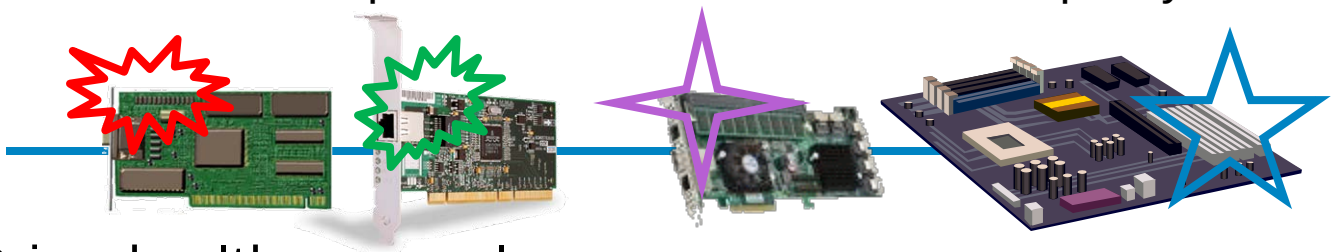
Updatable firmware:
EFI_FIRMWARE_MANAGEMENT_PROTOCOL (FMP)

- All adaptor firmware has some way of managing firmware
  - Get firmware version; Update the image; etc.
- Proprietary ways to common set of functions are not efficient
- FMP abstracts only the external interface, not the actual update logic
- FMP makes managing firmwares easy, allowing a common UI for all firmware updates
- FMP is required for Dell PowerEdge Servers

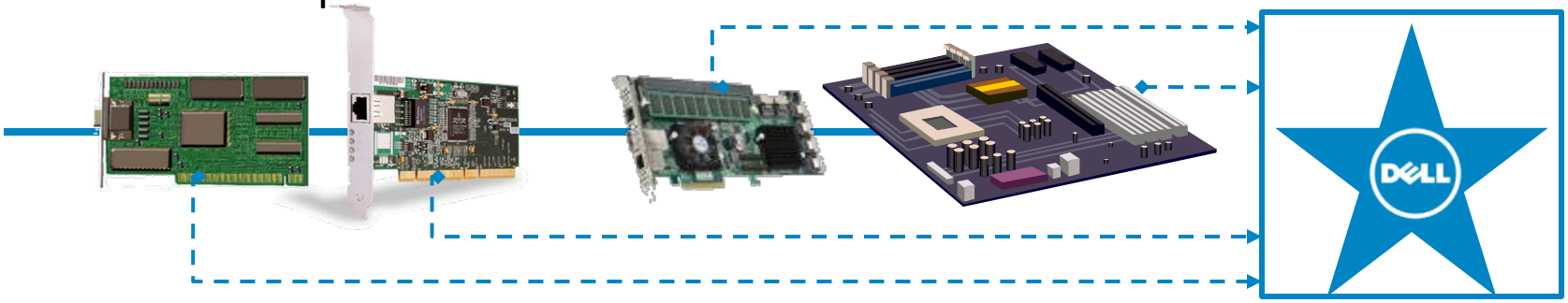


Error reporting and user interaction: EFI_DRIVER_HEALTH_PROTOCOL

- Issues with Current Error reporting model
  - POST flow interrupted every time
  - Errors on multiple devices could result in multiple system reboots



- Driver health protocol
  - Allows consolidation of all the error reporting and user interaction
  - Allows user to address all of the issues at the same time
  - Avoids multiple reboots



Storage

- Storage drivers must support >2.2 TB
- SCSI drivers must support EFI_EXT_SCSI_PASS_THRU_PROTOCOL:
- ATA drivers must support EFI_ATA_PASS_THRU_PROTOCOL

Global requirements

- Must be compliant with UEFI 2.3 spec
- Must certify with SCT
  - SCT - Self Certification Test. UEFI offer a complete suite to test your driver for UEFI compliancy

Agenda

- Review of IHV applicable UEFI features
- UEFI Benefits to IHVs
- Recommendations from Dell
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

Agenda

- UEFI Benefits to IHVs – LSI Corporation's Experience
  - UEFI Adoption Benefits
  - Faster Time to Market
  - Richer Capabilities
  - Enhanced Usability
  - Cost Savings

LSI UEFI Adoption Benefits

- LSI is a Contributor Member of UEFI Forum
- UEFI / HII is supported on all RAID HBAs
- LSI Customers (Major OEMs and ISVs) are already shipping 64-bit UEFI Platforms in Volumes
  - Leadership position among RAID HBA Vendors

Leadership in Enabling RAID HBA Customers

LSI UEFI Benefits - Faster Time To Market

- LSI Benefited from:
  - Industry adopted, Stable and fully Documented UEFI specifications
  - Readily available Development Kits / Reference Code and Platforms
  - Implementing **Modern** Firmware **Architecture** & **Ease** of Development
- UEFI SCT enabled LSI to provide:
  - **Quality** UEFI Option ROM Software for Test and Manufacturing
  - **Smoother** and Instant **integration** of LSI UEFI HII Drivers and OEM UEFI System Firmware

Faster Time to Market

LSI UEFI Benefits: Richer Capabilities

UEFI adoption enhanced LSI Feature Capabilities:

- UEFI provides **direct access** to all of (64-bit) Memory
- Ability to **quickly** implement new features and additional OEM requirements
- LSI UEFI HII Driver has:
  - Support for **"> 2.2 TB"** and **latest** Hard Disk technologies
  - **Unified** Interfaces across Option ROM Code
  - **Cleaner** and **Portable** Solutions
  - **Conformance** to Industry Standard Specs
- Support for **Hybrid** Systems -UEFI and Legacy BIOS

Faster Time to Market

LSI UEFI HII Benefits: Enhanced Usability

- HII allowed LSI to focus mainly on Functionality and Content rather than carrying own GUI so that:
  - OEMs can maintain their **own look-n-feel** across their platforms through their HII Browser
  - Standards based and **Customization** for RAID Configuration GUI at Build/Run Time
  - LSI solution allows OEMs to **differentiate** their Platforms from that of other OEMS
- Easier **Localization** Support
- Migration of Legacy BIOS / Utilities to single 64-bit cross platform UEFI HII Driver

LSI UEFI Benefits: Cost Savings

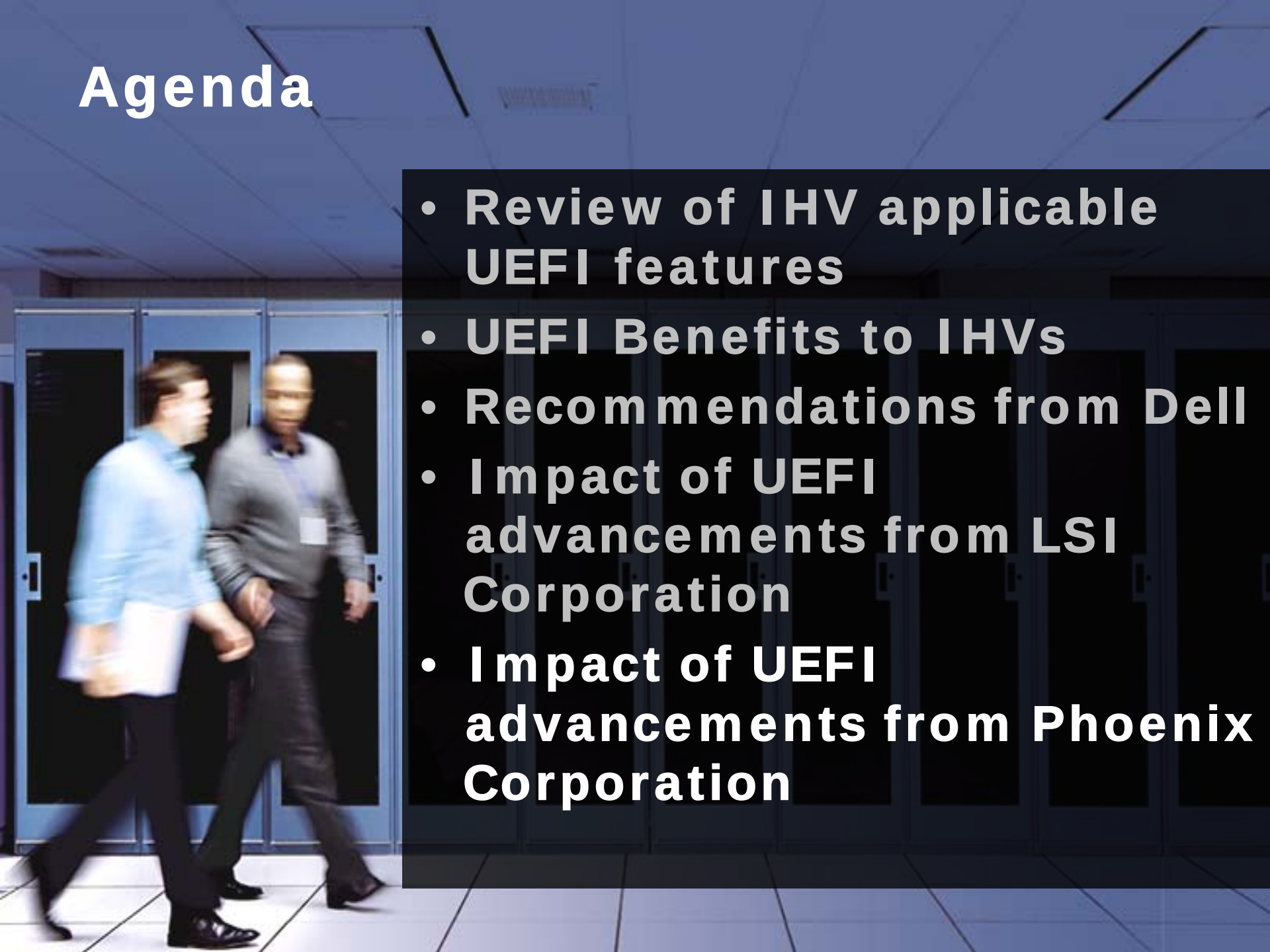
- '**C**' Language Development Environment and Proven Tools and EDK
- Stable and **re-usable** Code base and **less** chance of errors / **defects**
- Easier to Test and **Debug** - Local & Remote
- Higher **Quality** Option ROM Code means Faster Deployments for multiple OEMs
- Improved overall **efficiency** resulting in **Lower** Development and Maintenance **Costs**

Lower Development Costs

LSI UEFI Benefits Summary

- Leadership among RAID HBA Vendors
- Faster Time to Market
- Cost Savings
- Richer Capabilities
- Enhanced Usability

Agenda



- Review of IHV applicable UEFI features
- UEFI Benefits to IHVs
- Recommendations from Dell
- Impact of UEFI advancements from LSI Corporation
- Impact of UEFI advancements from Phoenix Corporation

IBV Viewpoint – Why UEFI?

- Why should IHVs migrate to UEFI Option ROMs?
  - For block devices, disks > 2.2TB are not supported as boot devices
  - Too many limitations to list
  - Boot speed
    - Legacy real-mode OpROMs are slower than properly implemented UEFI option ROMs
    - Most devices with legacy OpROMs must be initialized even if not needed for boot
    - Phoenix provides a smart implementation that learns how to optimize boot based on history and customer configured profiles

UEFI is not only desirable…

- Eventually, OEMs will no longer support legacy Option ROMs (sooner than you think)
  - You may not be eligible for inclusion in OEM systems if you don't have UEFI OpROM support
  - Your add-in devices will no longer work on legacy free systems
- UEFI provides a standard approach to User Identification and Profiles for security
  (see Chapter 31 of the UEFI 2.3 spec.)
- Friendly/portable human interface
  - You don't have to carry your own UI in your code
  - See next page for example

HII Browser Example

Phoenix and LSI are working on getting a screen shot or two with the Phoenix SecureCore Tiano™ browser. They will go here when available.

Independent BIOS Vendor Assistance for developers

- Optional protocols typically required
  - Pass thru protocols for block devices (i.e. ATA/ATAPI devices) are needed to enable some drive functionality
- How Phoenix can help
  - We have developed UEFI option ROMs for many IHVs (in house expertise/experience)
  - Would a Phoenix supported OpROM SDK be of value to you?
  - We are happy to work with you to leave legacy behind

phoenix technologies

Summary

- UEFI features provide IHVs a simple, powerful method to describe device configuration data and health status
- Dell sees huge value in UEFI, Optional UEFI protocols are recommended by OEMs
- UEFI provides cost savings, faster time to market, and flexibility
- Migrate to UEFI as legacy option ROM support deprecates

Additional sources of information on this topic:

- Other Sessions – Next Slide
- Demos in the showcase – #160
- Additional info in the SSG community – EFI Booth
- More web based info:
  - ***UDK 2010 - http://www.tianocore.Sourceforge.net***
  - ***UEFI Specifications - http://www.uefi.org***
- Book on topic:
  - Beyond BIOS 2nd edition - Intel Press

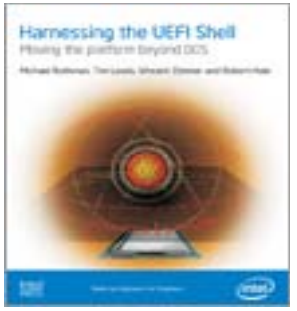
IDF 2010 UEFI Fall Sessions
Sept. 13, 2010 Moscone Room 2006

EFI#	Company	Description	Time
✓ S001	Intel, IBM, HP	Introducing the New Intel® UEFI Development Kit: Industry Foundation for Platform Innovation	11:00 AM
✓ S002	Intel, LSI, Dell, Phoenix	UEFI Advancements for Independent Hardware Vendors	1:05 PM
S003	Intel, WindRiver	Boot Loader Solutions for Intel® Atom™ Processor Based Embedded Devices	2:10 PM
S004	Intel, Dell, AMI	Zero-Touch Platform Manageability with UEFI	3:15 PM
S005	Intel, IBM, Insyde	Beyond DOS: The UEFI Shell – a Modern Pre-boot Application Environment	4:20 PM
Q001	All	UEFI Q & A session with all Speakers	5:25 PM

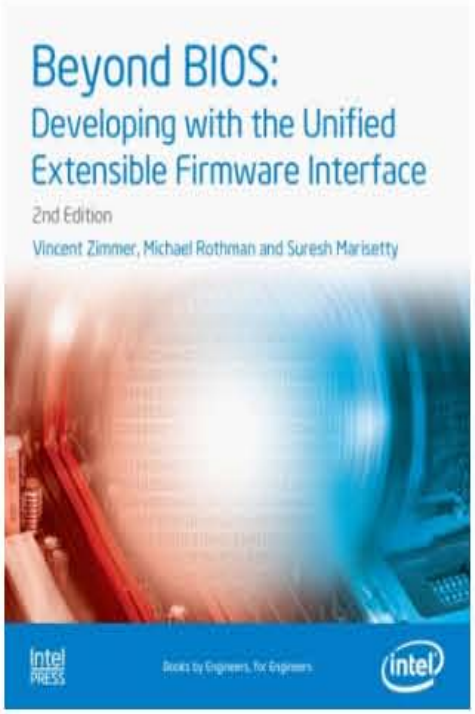
✓ DONE

Call to Action / Next Steps: UEFI Resources for IHVs

- Visit UEFI Forum – http://uefi.org
  - Become a Member
  - Download latest UEFI Specifications, including
    - UEFI Driver Writer's Guide
    - UEFI Shell
    - HII Documentation (Part of UEFI Spec)
- Visit Tianocore – http://tianocore.sourceforge.net
  - Download Development Kits and Test Suites
    - UEFI EDK / EDK II / UDK 2010
    - UEFI SCT
- Visit Intel Press for UEFI Books – http://intel.com/intelpress



Beyond BIOS 2nd edition promotion



2nd Edition - *Beyond BIOS* available Q4 2010

To receive a complementary copy of the book Register at http://www.intel.com/intelpress/register.htm

Enter "Beyond BIOS Offer" plus the serial number on the back of this voucher in the Book Title field. Your book will be shipped to you.

Offer not valid for Intel employees. Limited time offer.

Vouchers available in session room and EFI tech showcase booth

UDK2010 Available on tianocore.org

tianocore.org

UDK2010
Open Source
UEFI Development Kit

Develop. Contribute. Advance.

http://www.tianocore.Sourceforge.net

IDF 2010 UEFI Fall Sessions
Sept. 13, 2010 Moscone Room 2006

EFI#	Company	Description	Time
✓ S001	Intel, IBM, HP	Introducing the New Intel® UEFI Development Kit: Industry Foundation for Platform Innovation	11:00 AM
✓ S002	Intel, LSI, Dell, Phoenix	UEFI Advancements for Independent Hardware Vendors	1:05 PM
S003	Intel, WindRiver	Boot Loader Solutions for Intel® Atom™ Processor Based Embedded Devices	2:10 PM
S004	Intel, Dell, AMI	Zero-Touch Platform Manageability with UEFI	3:15 PM
S005	Intel, IBM, Insyde	Beyond DOS: The UEFI Shell – a Modern Pre-boot Application Environment	4:20 PM
Q001	All	UEFI Q & A session with all Speakers	5:25 PM

✓ 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/idfsessions

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 PROPETY 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 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.
- UDK2010 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, Intel® UDK 2010, 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 second 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 the flash memory market segment, and declines in this market segment or changes in management's plans with respect to our investment 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 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 March 27, 2010.

Rev. 5/7/10

Backup Slides