Intel® UEFI Development Kit 2010 and Intel® Boot Loader Development Kit: Foundations for Advanced Embedded Development

Alex Gu, Engineering Manager, Intel
Jason Jin, Technical Marketing Engineer, Intel

EFIS004

Sponsors of Tomorrow.™ intel

Agenda

- Intel® UEFI Development Kit 2010 Key Features
- Embedded Device Boot Loader
- Intel® Boot Loader Development Kit Key Features
- Summary

Agenda

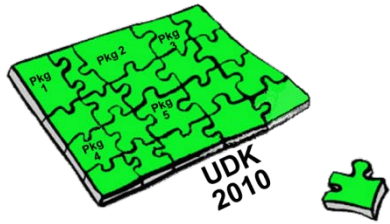
- Intel® UEFI Development Kit 2010 Key Features
- Embedded Device Challenges
- Intel® Boot Loader Development Kit Key Features
- Summary

Intel® UDK2010 Enables a Common Firmware Development Foundation Across the Compute Continuum

Spotlight on Select Intel® UDK2010 Features

- UEFI Specification Support
- Packaging
- Multiple compilers and OS development environment support
- Platform Configuration Database
- Well defined and Optimized Libraries
- Source Level Debugger
- Security
- IP6 Networking

UEFI Specification Support



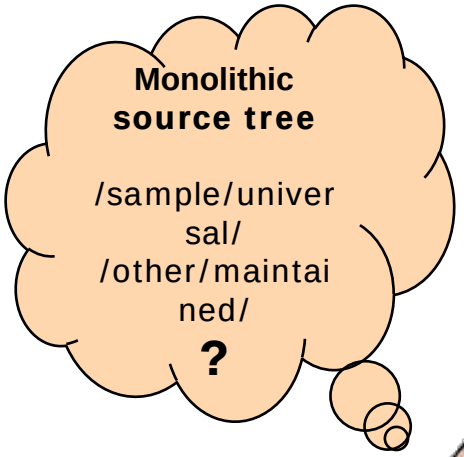
- Intel® UDK2010 Native support:
  - UDK2010 includes support for UEFI 2.2, UEFI 2.3, PI 1.1, and PI 1.2 (as well as all previous UEFI, EFI, and PI Specifications)
    - Shell 2.0 specification support in separate shell package
  - Pre-UDK contained definitions for UEFI 2.0, UEFI 2.1, PI 1.0 and Framework 0.9x Specifications; focused on UEFI 2.1 and PI 1.0 (PEI Core, DXE Core, PEIMs, DXE Drivers, UEFI Drivers, and libraries)

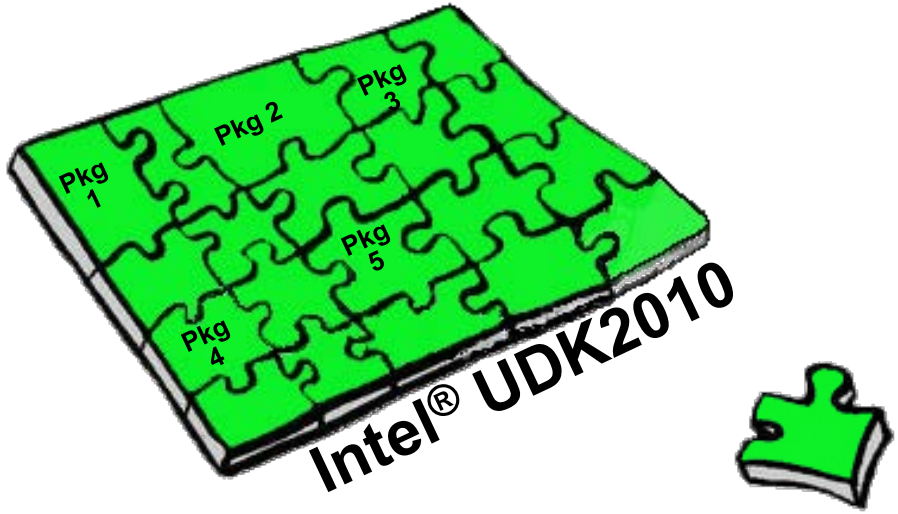
Security / Networking - UEFI 2.3
- IPV6/IPSec – next gen internet IP address allocation and security
- User Authentication & Driver Signing
- iSCSI & VLAN

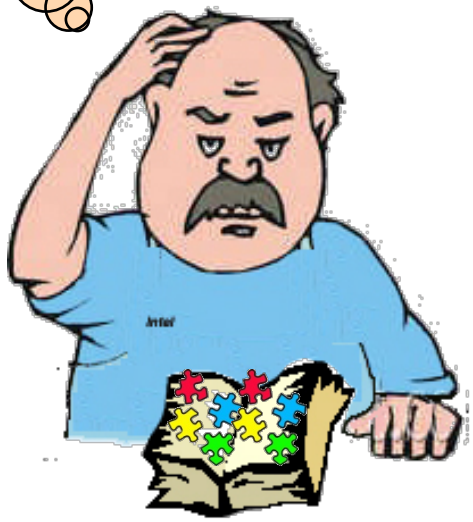
Human Infrastructure Interface (HII) – UEFI 2.1

Advanced Standard-based Capabilities

Packaging: Enabling Fast Delivery of Advanced Capabilities to Market







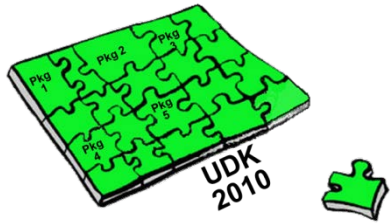
Firmware Developer

Example of Package-based deployment

- **Package 1** Industry standard modules and drivers
- **Package 2** Chipset PEIM's and DXE drivers
- **Package 3** System board code
- **Package 4** OEM Value-add

Intel® UDK2010 enables all the pieces to fit together and work!

Multiple Compilers and OS Development Environment Support Improvement over EDK

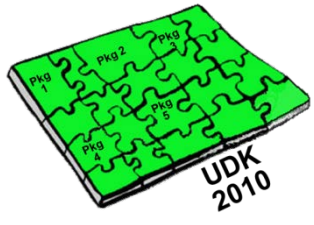


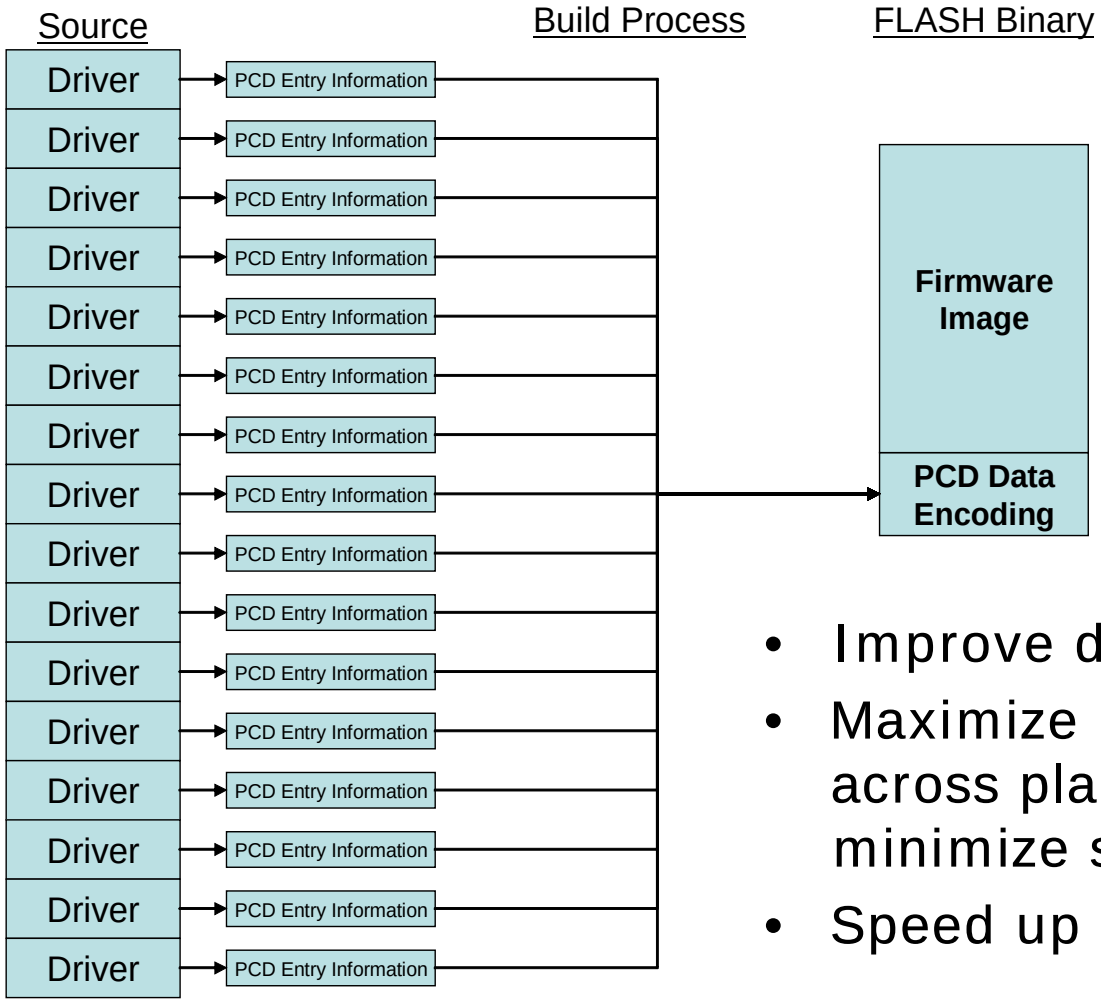
	EDK	UDK 2010
Development OS	Windows* XP	Windows XP, Windows 64, Vista32, Vista64, Linux*, OS/X*
Compiler/Linker	Visual Studio 2003, 2005, WinDDK	Visual Studio 2003, 2005, 2008*, WinDDK*, Intel® C++Compiler, GCC
Build	nmake	nmake, gmake
Build Tools	C	POSIX C, Python*

Improved Features and Support

GCC GNU Compiler Collection for C++
POSIX C Portable Operating System Interface for Unix

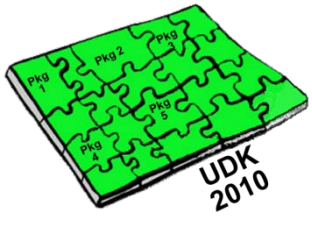
Platform Configuration Database

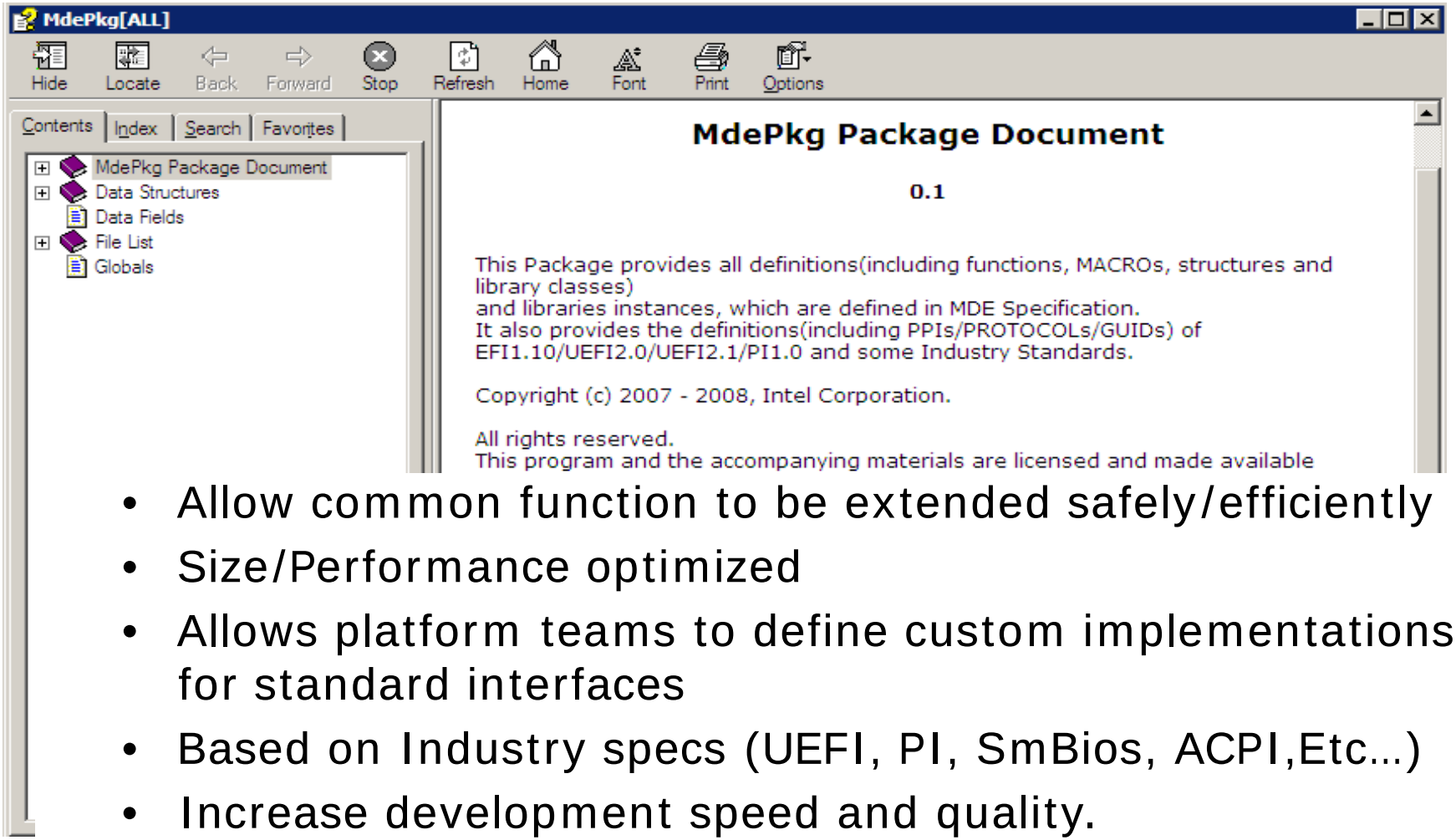




- Improve developer efficiency
- Maximize modules reuse across platforms and minimize source code editing
- Speed up development

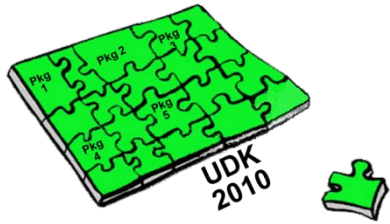
Optimized Libraries





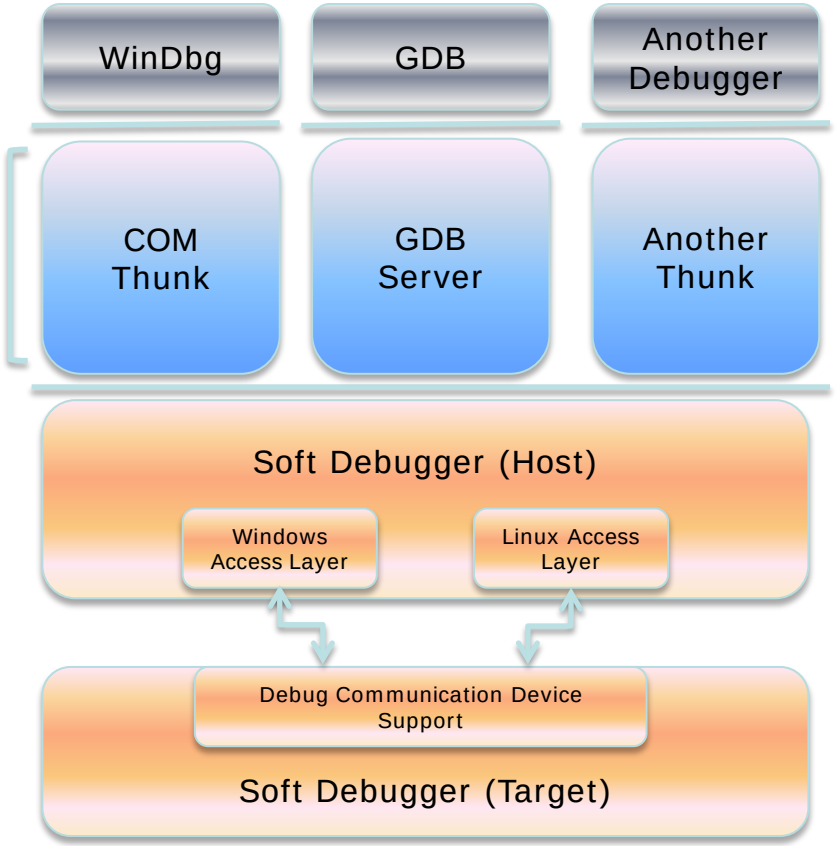
- Allow common function to be extended safely/efficiently
- Size/Performance optimized
- Allows platform teams to define custom implementations for standard interfaces
- Based on Industry specs (UEFI, PI, SmBios, ACPI,Etc…)
- Increase development speed and quality.

Source Level Debugger



The Intel® UDK2010 contains a Source Debugger Package:

- Interface and use like the standard Windows* WinDBG* tool
  - Low learning Curve
  - Robust operation
  - Support from early pre-boot phase
- Integrated directly into the Pre-boot image of the platform
- Uses Serial or USB port for communications to host platform



Intel® UDK2010 Available on tianocore.org

tianocore.org

Intel® UDK2010
Open Source
UEFI Development Kit

Develop. Contribute. Advance.

http://www.tianocore.Sourceforge.net

Agenda

- Intel® UEFI Development Kit 2010 Key Features
- **Embedded Device Boot Loader**
- Intel® Boot Loader Development Kit Key Features
- Summary

Embedded Growth Today and Future

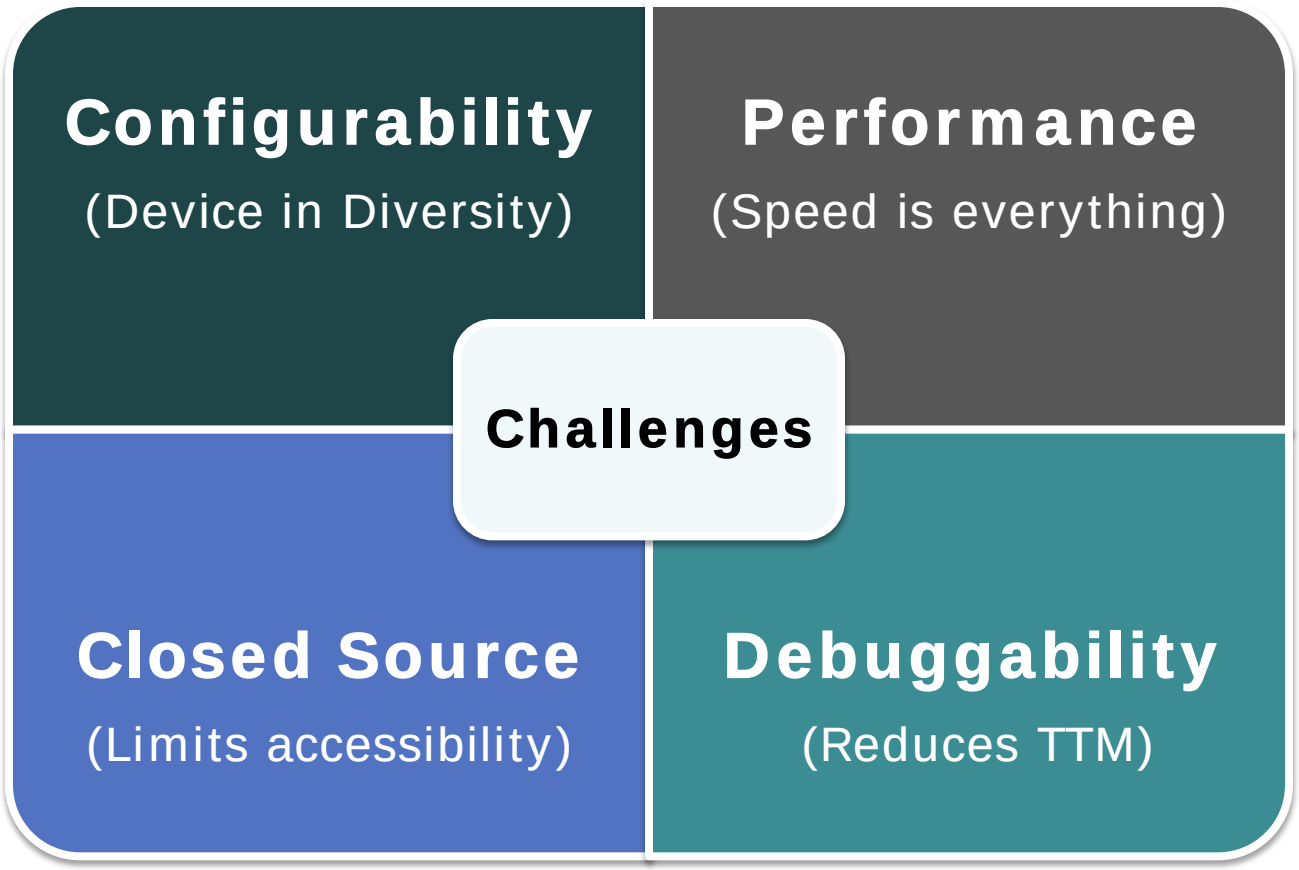
Embedded market is growing rapidly in diversity

Traditional BIOS vs. Embedded Boot Loader

BIOS Dynamically configures per Broad PC industry standards	Boot Loader Statically configures for a specific application
• Standard OS compatibility • Feature richness • Open to many use cases • Multiple boot paths • Extra services and support • For a price	• Custom OS & applications • Basic IA initialization • Quick and small • Single use case • Limited boot options • No frills • Royalty free • No hand-holding

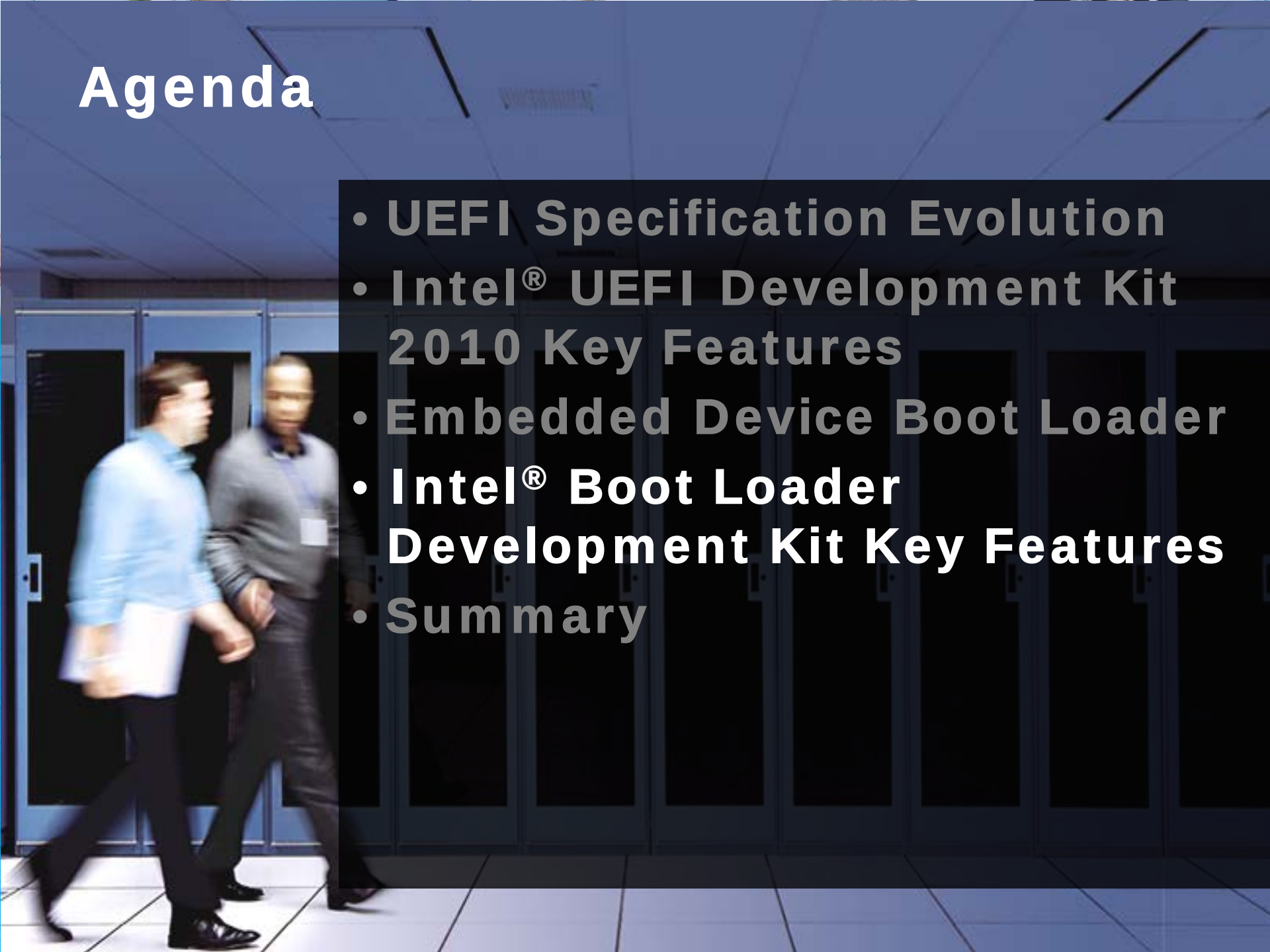
Intel® BLDK is designed for Embedded Boot Loader

Embedded Device Boot loader Challenges



Intel® UDK2010 can address these challenges

Agenda



- UEFI Specification Evolution
- Intel® UEFI Development Kit 2010 Key Features
- Embedded Device Boot Loader
- **Intel® Boot Loader Development Kit Key Features**
- Summary

Intel® Boot Loader Development Kit

Documentation & Sample Reference Code

- Comprehensive instructional documents enable Self-Sufficiency and effective, scalable support

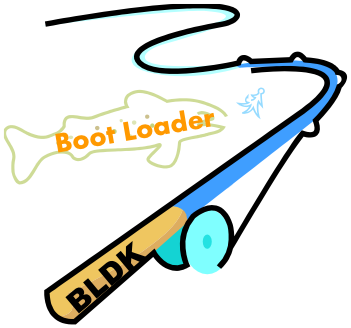
CRB Example Image & Firmware Code

- Example Intel CRB Image & BOM provides baseline from which customers can modify their system firmware image

Software Tools and GUI Interface

- GUI Module Selection & Build Tool allows custom image creation without direct code changes
- IDE facilitates Easy Navigation and Modification of the Code

Intel BLDK provides the mechanism for customers to develop their own boot loader solutions



Intel BLDK is on http://goto.intel.com/bldk

Intel® BLDK Key Features

Industry Standard Compliant
- UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3 and PI 1.0, PI 1.1, PI 1.2
- ACPI 3.0

Customer Binary Configuration
- Feature selection and binary patchable without direct code change

Multiple Tools Chains Support
- MSFT (VS2003, VS2005, VS2008, WinDDK), GNU (GCC), INTEL (ICC)

Multiple Boot Device
- Boot from ATA, SSD, CF, SD, USB, FWH, SPI, iSCSI, PXE

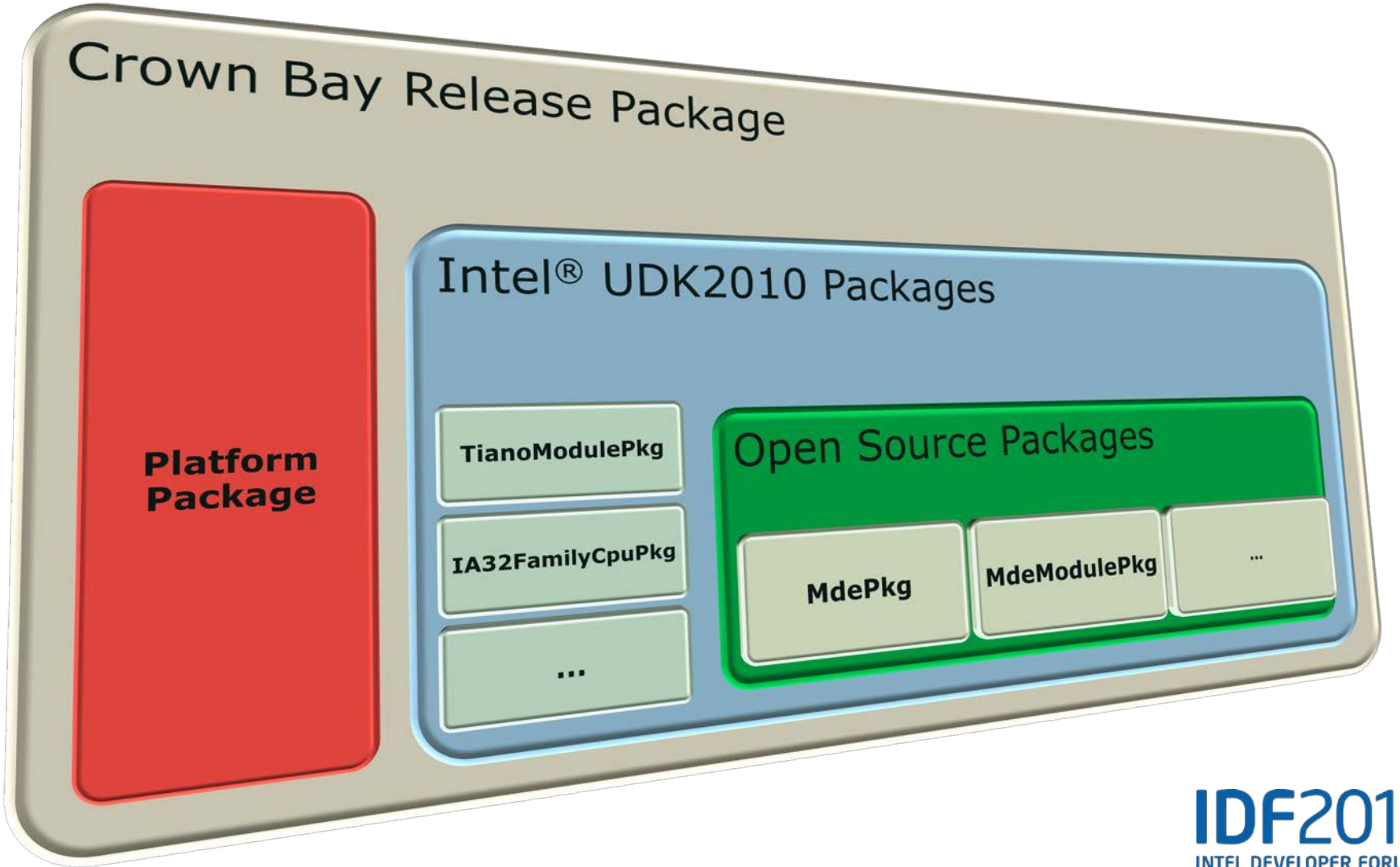
Source Level Debug
- UDK Debugger Tool provide pure soft debug solution

Extensible Foundation
- Pre-OS Security, Rich Networking, Manageability, etc.

Royalty-free Source Code
- Majority of source available via tiano.org

Intel® UDK2010 is the best choice of firmware code

Intel® Atom™ Processor E6xx Series with Intel® Platform Controller Hub EG20T Platform (Codename Crown Bay) – Based on Intel® UDK2010



Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Address Challenge – Configurability

- Configurability is a key feature in embedded
  - Ability to customize behavior and optimize for the target environment involves what might be some changes to the normal desktop PC behavior model.
  - Is there a UI to launch?

Interactive Boot

No pre-boot interaction

  - What type of hardware are we required to initialize prior to launching the payload?

The embedded space has some unique policy decisions

Address Challenge - Performance

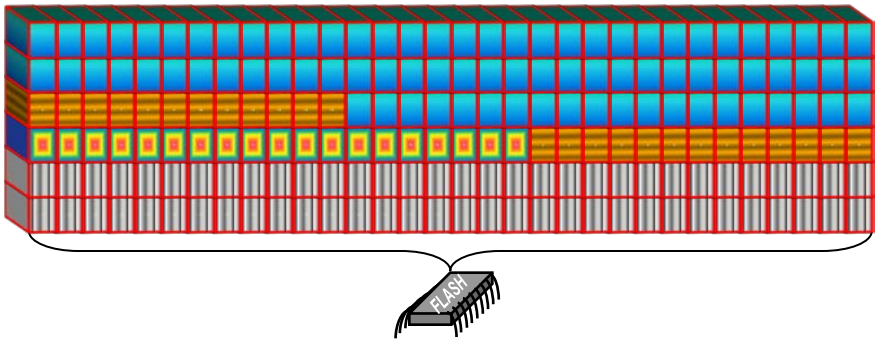
- Boot Target Hardware Choice
  - Boot device spin-up/down time affects performance
  - Use of an SSD boot device in lieu of rotating media can save seconds in the boot time

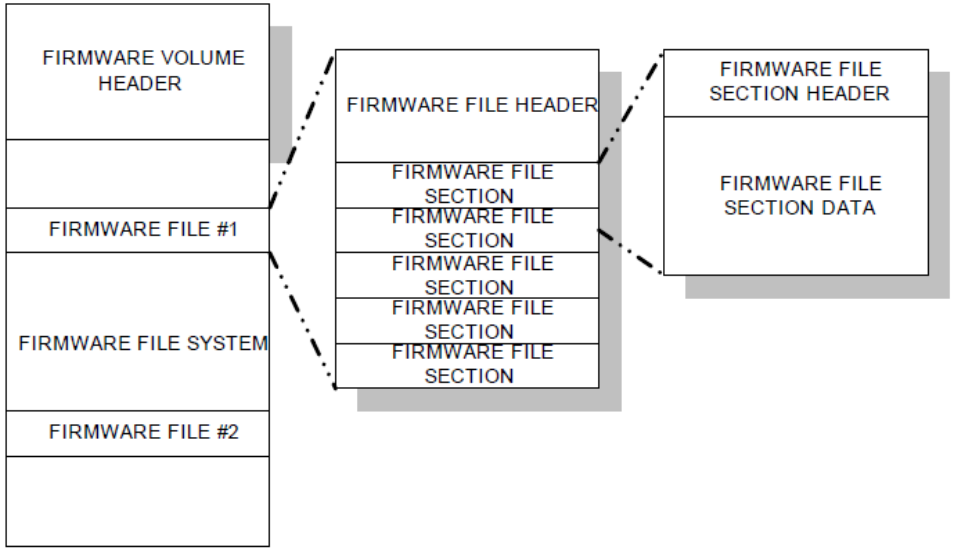
Values	DRAM	SSD (34nm)	EIDE
Read Latency	~30 ns	65 µs	8.5 ms
Read BW (MB/s)	1800	250	120
Write Latency	~30 ns	85 µs	10 ms
Write BW (MB/s)	1800	70	120
Spin-up/down time	N/A	N/A	1-2s++

The shorter boot device legacy, the faster boot time

Address Challenge – Performance (Cont)

- FLASH Organization
  - Flash layout affects performance
  - Organize FLASH layout so that you only search firmware volumes which contain items of interest for that configuration





Core Firmware Components (e.g. SEC/PEI Core/DXE Core)

Firmware Data (e.g. Drivers for certain configurations)

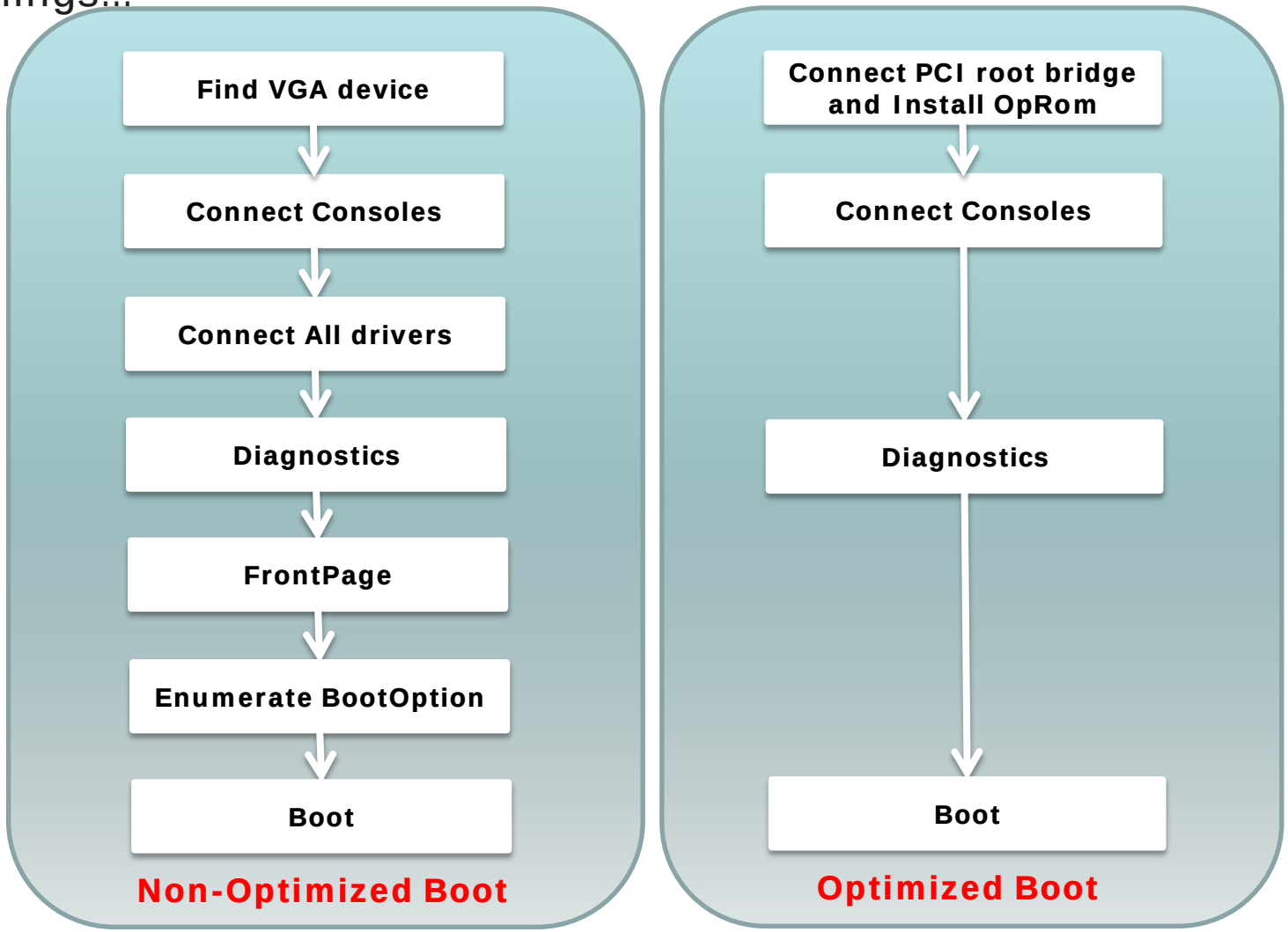
Alternate Firmware Data (e.g. Drivers for other configurations)

Free Space

The more organized layout, the faster boot time

Address Challenge – Performance (Cont)

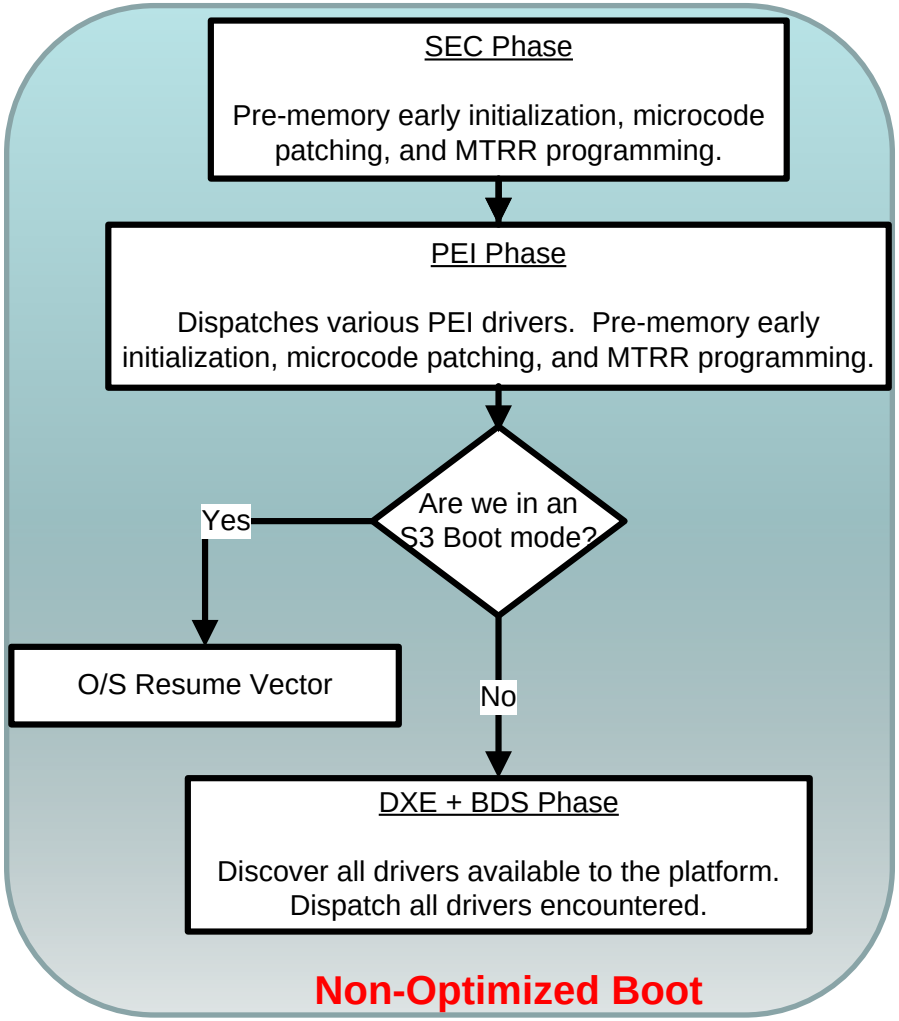
- Note that depending on platform needs, we may very well do different things…

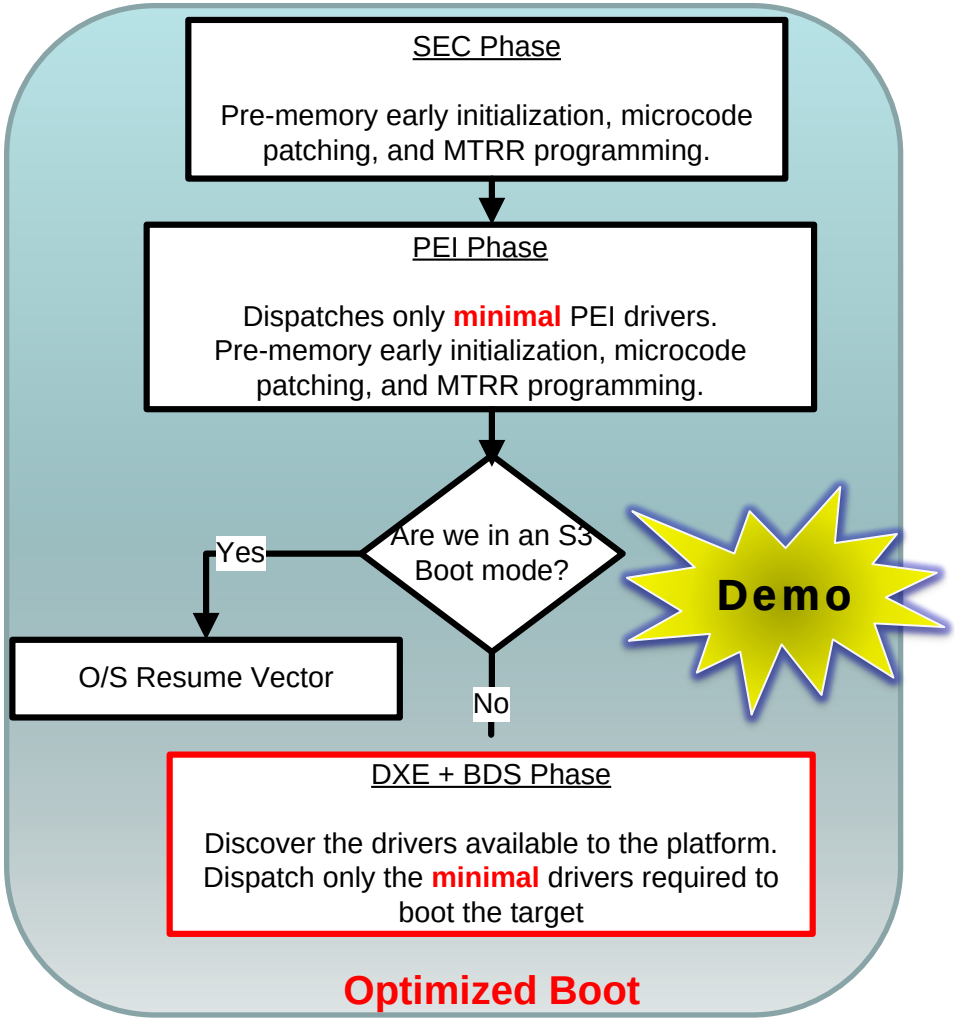


The more customized boot sequence, the faster boot time

Address Challenge – Performance (Cont)

- Performance Optimization doesn't mean we lose UEFI compatibility



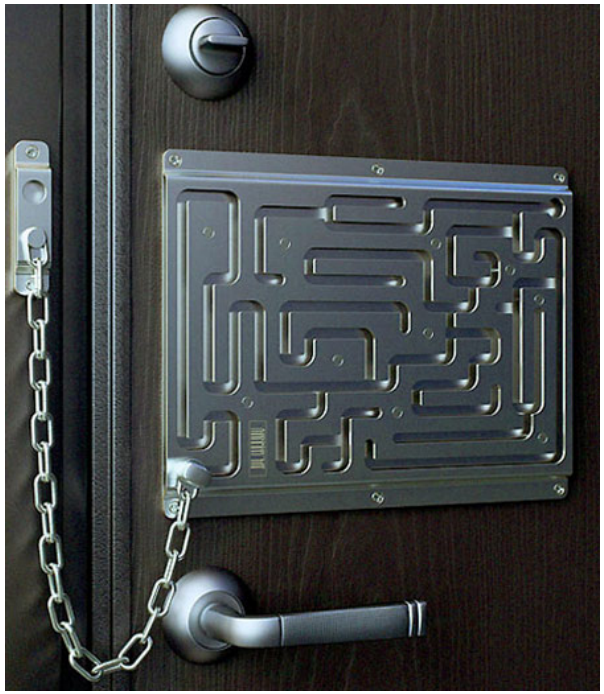


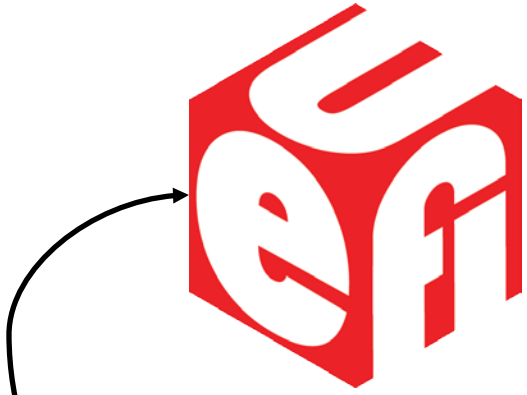
More details in a whitepaper located at: http://edc.intel.com/Link.aspx?id=4603

Optimize without losing UEFI compatibility

Address Challenge – Closed Source

- Limited access to certain source material
  - Traditionally, closed source code and distribution restrictions in a Boot Loader has made distribution to a wide audience a challenge.





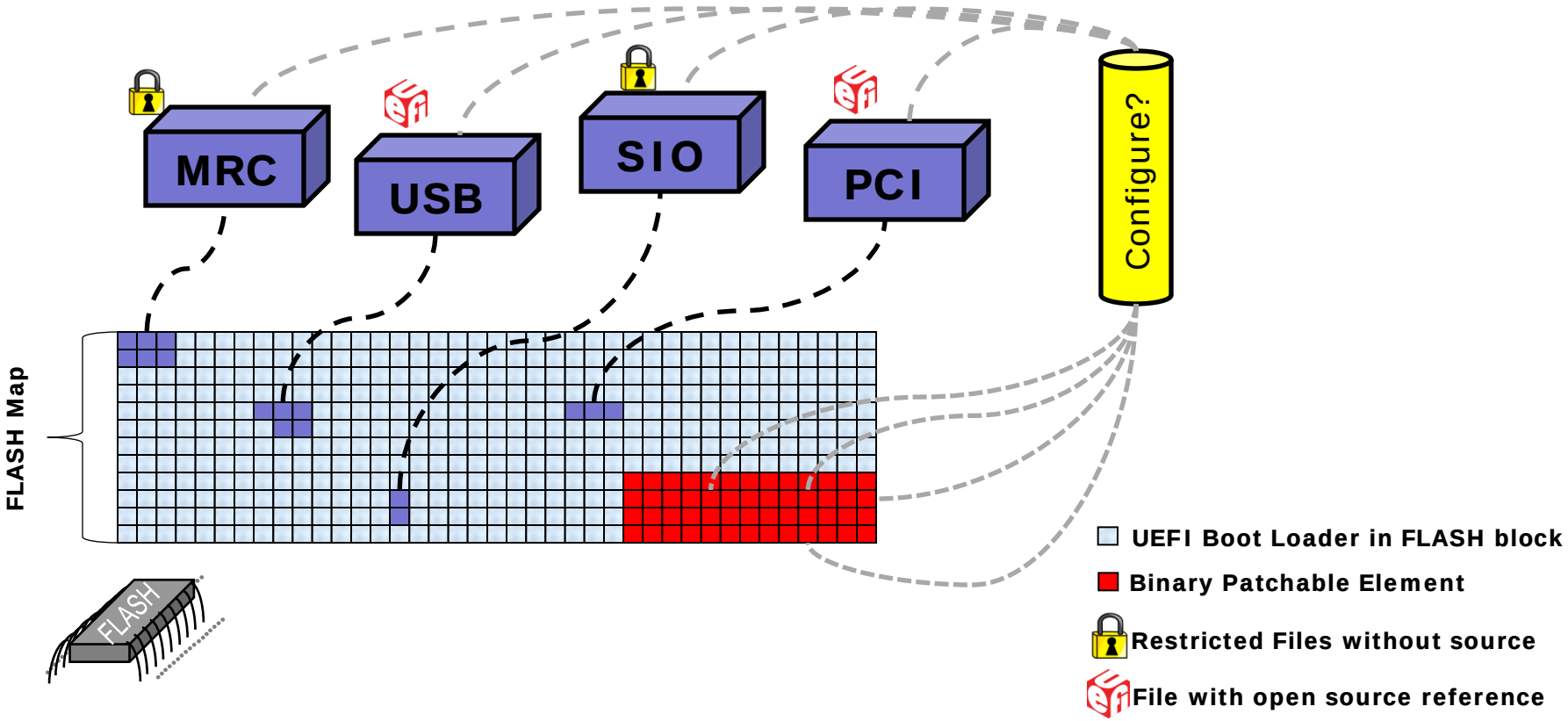
www.tianocore.org forwards user to a Source Forge repository.

Relatively small portion remains With source & distribution restrictions

UEFI introduces a large amount of open source

Address Challenge– Closed Source (Cont)

- By extending the configurability of binary components, we can enable much broader usage.



Binary image manipulation removes source restriction hurdles so a large variety of clients can use solution

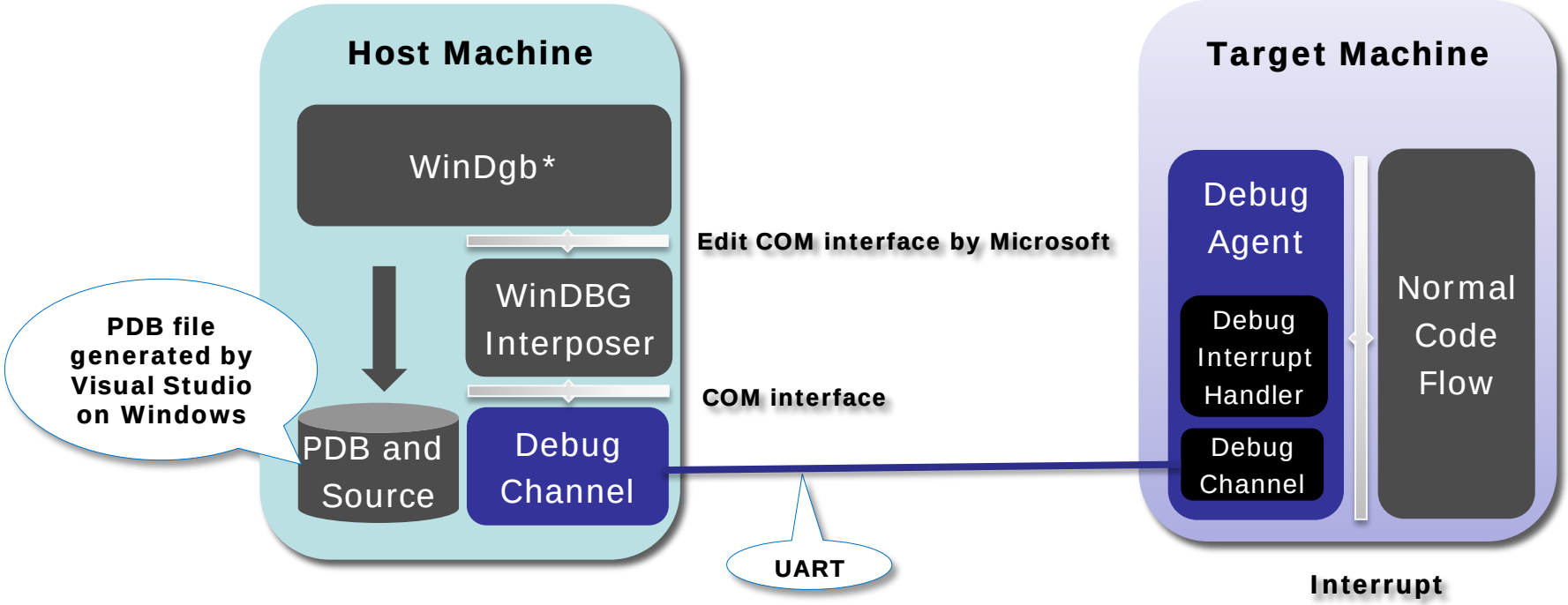
Address Challenge – Debuggability

- Software-only debugger solution
  - New Intel® UEFI Development Kit Debugger Tool available
  - Provides ability to debug target without need for exposed JTAG
    - Leverage various debug ports (e.g. USB, Serial)
  - Supports WinDbg* as a front-end
  - Few differences between this solution and a high-end HW-based debugger
    - To break into target, SEC startup code must have established a stack.
      - Typically a few dozen instructions from the reset vector.
      - This is also true of first few dozen instructions in SMI entry.
    - Some Processor mode transitions are difficult to debug.

UEFI-based open source debugger solutions available

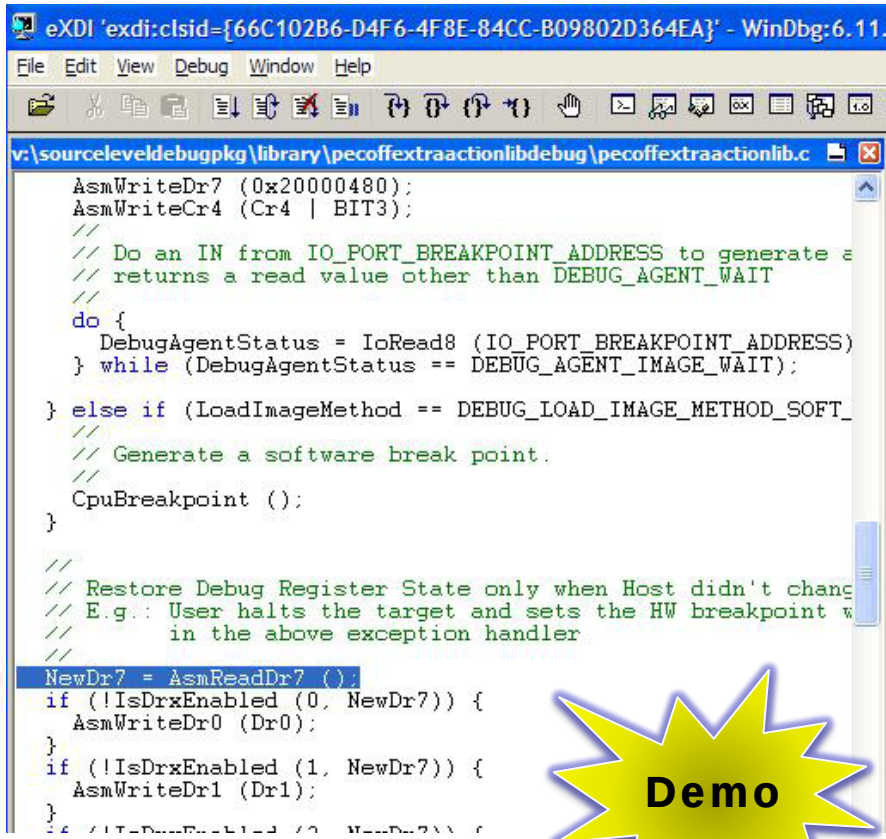
Address Challenge – Debuggability (Cont)

- Intel® UEFI Development Debugger Tool Architecture



Address Challenge – Debuggability (Cont)

- WinDBG* should stop the TARGET at late SEC phase, and loaded the symbols for SecCore. WinDbg will show the source code similar to the example shown
- Bottom window allows commands to be entered
  - .reboot
  - Smmentrybreak=1 or 0
  - g - Go
  - B[C|D|E][<bps>] - clear/disable/enable breakpoint(s)
  - Q - quit
  - ? – Command list



Summary

- Intel® UEFI Development Kit 2010 (Intel® UDK2010) meets newest Industry Standard and provide a well suited development base
- Intel® Boot Loader Development Kit (Intel® BLDK) offers a solution to develop Intel® Atom™ Processor based embedded design rapidly.
- Intel UDK2010 is the best choice of firmware to help Intel BLDK to address embedded design challenges.

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

EFI Track Sessions

Session ID	Title	Day/ Time	Room
✓ EFIS001	Microsoft* Windows* Platform Evolution and UEFI	Tuesday 11:10	306A
✓ EFIS002	UEFI Development and Innovations for System-On-Chip (SoC)	Tuesday 14:05	306A
✓ EFIS003	UEFI and Transparent Computing Technology	Tuesday 15:10	306A
✓ EFIS004	Intel® UEFI Development Kit 2010 and Intel® Boot Loader Development Kit: Foundations for Advanced Embedded Development	Tuesday 16:10	306A
SPCQ001	Hot Topic Q&A: Intel® Boot Loader Development Kit (Intel® BLDK)	Tuesday 17:00	306A
EFIS005	Security and Networking Advancements Today's UEFI and Intel® UEFI Development Kit 2010 (Intel® UDK2010)	Wednesday 11:10	306A

✓ = 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 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.
- Tunnel Creek, Crown Bay 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
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel, Atom, Atom inside, Core, Core inside, Xeon, Xeon inside, Sponsors of Tomorrow. 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 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. Revenue and the gross margin percentage are affected by the timing of 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 capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; product mix and pricing; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. 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 Intel's 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 Intel's 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 Intel's ability to design its 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 September 25, 2010.

Rev. 1/13/11

Backup Slides