Reshaping the Intel® Architecture Firmware Landscape using Intel® Boot Loader Development Kit (Intel® BLDK) for Embedded Designs

Drew Jensen

Firmware Product Marketing Manager

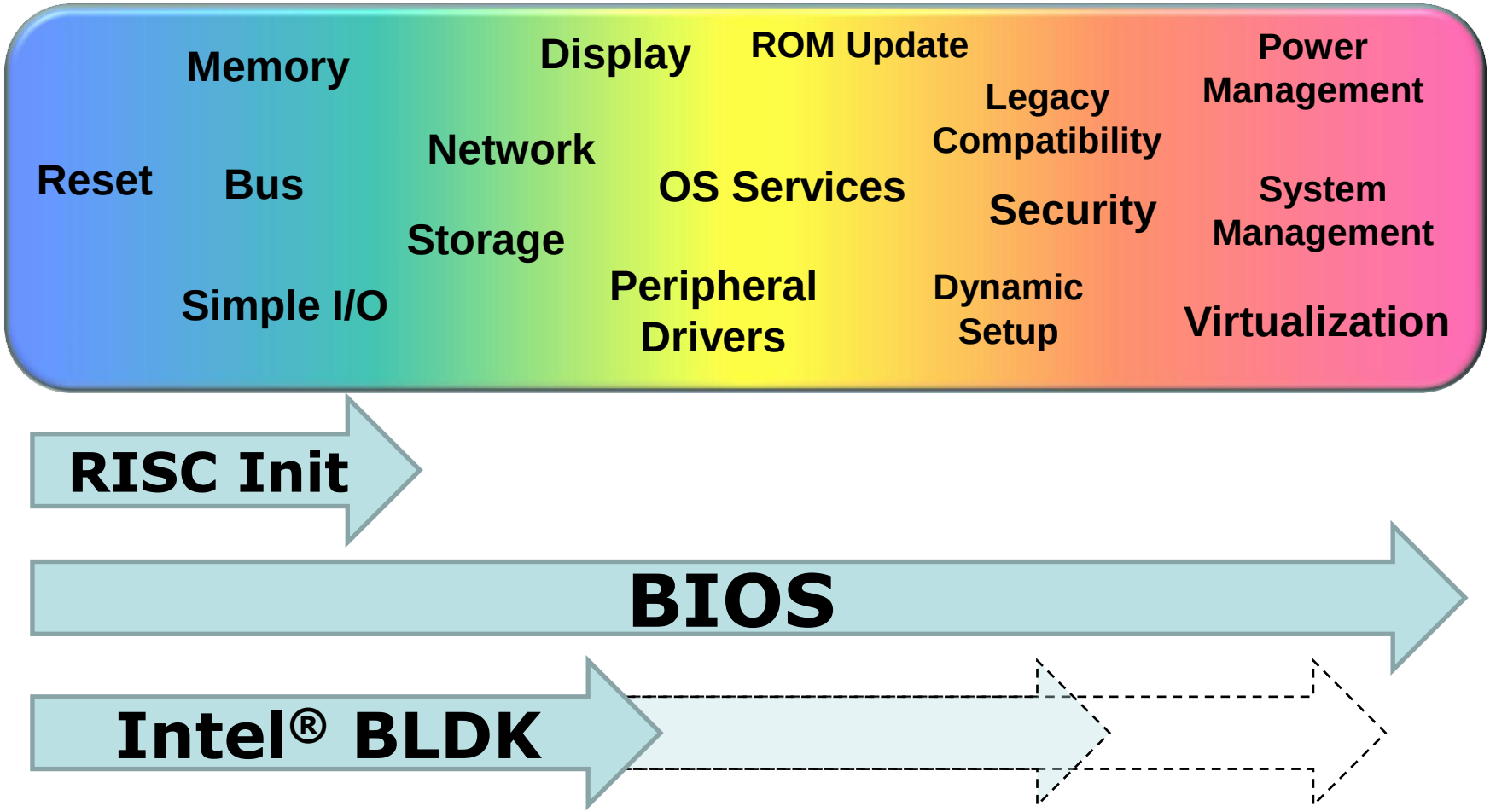
Agenda

- **Introduction to the Intel® Boot Loader Development Kit (Intel® BLDK)**
- **Features and Capabilities of Intel BLDK**
- **Firmware Customization and Optimization**
- **Debugging with Intel BLDK**
- **Q & A**

Agenda

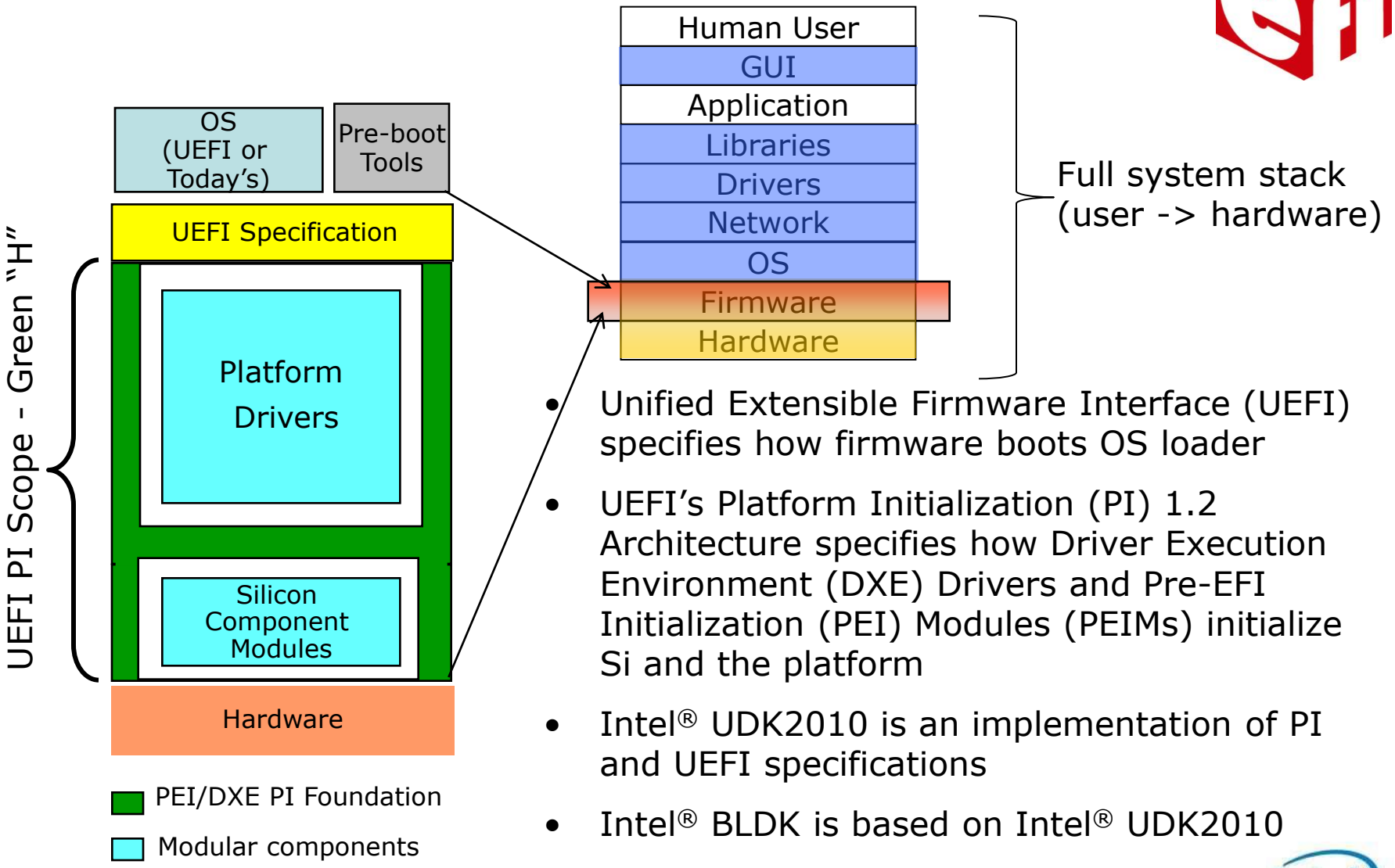
- **Introduction to the Intel® Boot Loader Development Kit (Intel® BLDK)**
- **Features and Capabilities of Intel BLDK**
- **Firmware Customization and Optimization**
- **Debugging with Intel BLDK**
- **Q & A**

Spectrum of System Initialization Firmware



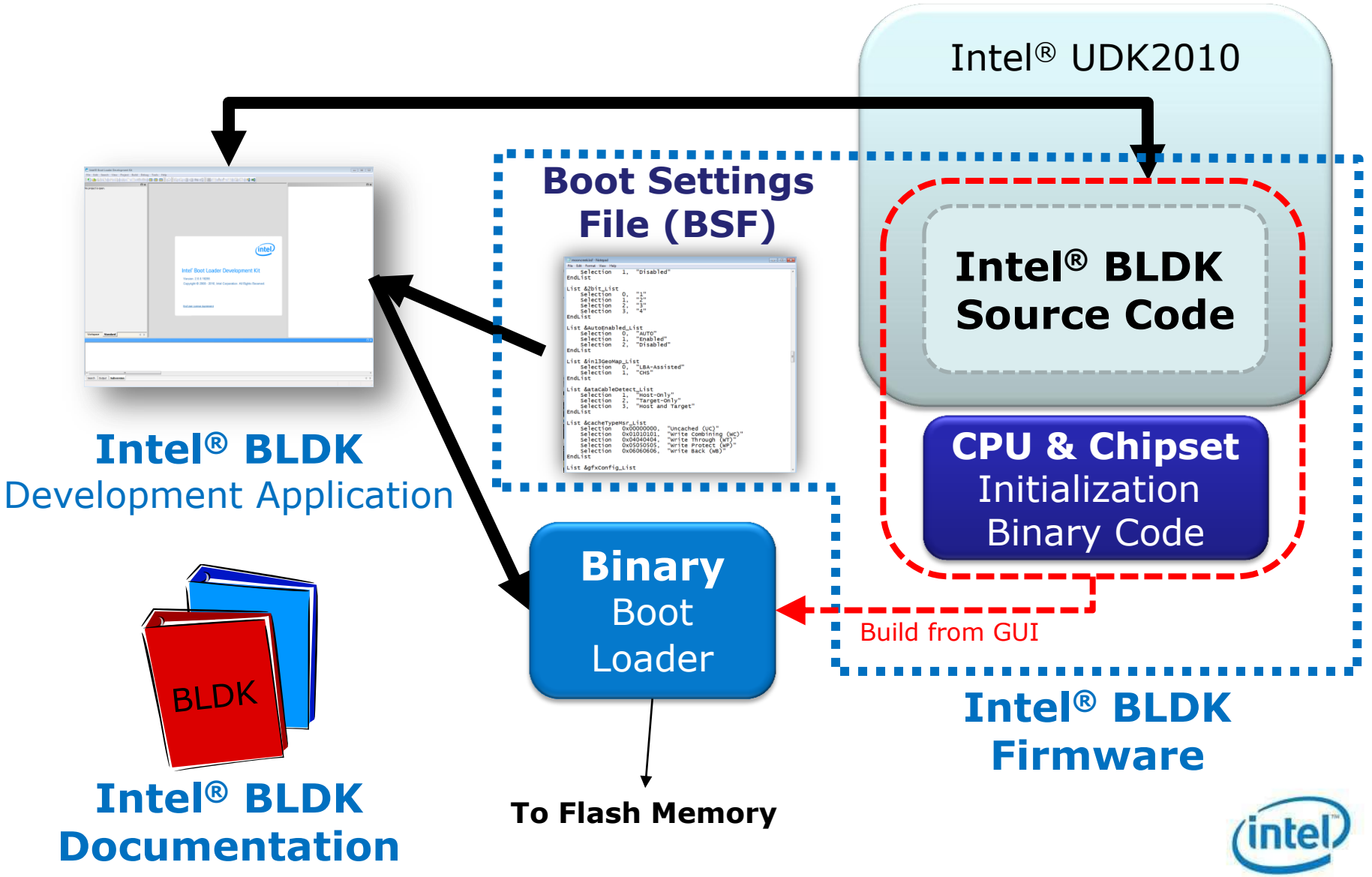
Intel® BLDK Provides Flexibility to Scale System Initialization for Embedded Systems

UEFI Platform Initialization Overview



- Unified Extensible Firmware Interface (UEFI) specifies how firmware boots OS loader
- UEFI's Platform Initialization (PI) 1.2 Architecture specifies how Driver Execution Environment (DXE) Drivers and Pre-EFI Initialization (PEI) Modules (PEIMs) initialize Si and the platform
- Intel® UDK2010 is an implementation of PI and UEFI specifications
- Intel® BLDK is based on Intel® UDK2010

Intel® BLDK Components



Embedded

Agenda

- Introduction to the Intel® Boot Loader Development Kit (Intel® BLDK)
- **Features and Capabilities of Intel BLDK**
- Firmware Customization and Optimization
- Debugging with Intel BLDK
- Q & A

Features of Intel® BLDK

Supported

- CPU, Memory, Basic IO Initialization
- Native UEFI Boot from SATA, SD, USB
- Feature configuration via Development Application
- Target OS: Windows* CE, Linux*, UEFI Shell
- Windows* and Linux* Tool Chains for development
- UEFI Specification 2.3 & PI Specification 1.2
- Fast Boot < 3s
- TCP/IP File Transfer
- ACPI 3.0
- Intel® UDK Debugger Tool
- Virtualization
- HD Audio

Not Supported

- Legacy Operating Systems
- Operating System Boot via Int19h
- Legacy USB
- Compatibility Support Module
- Intel® Active Management Technology
- Intel® Trusted Execution Technology
- Intel® vPro™ Technology
- Custom Remote Access Services

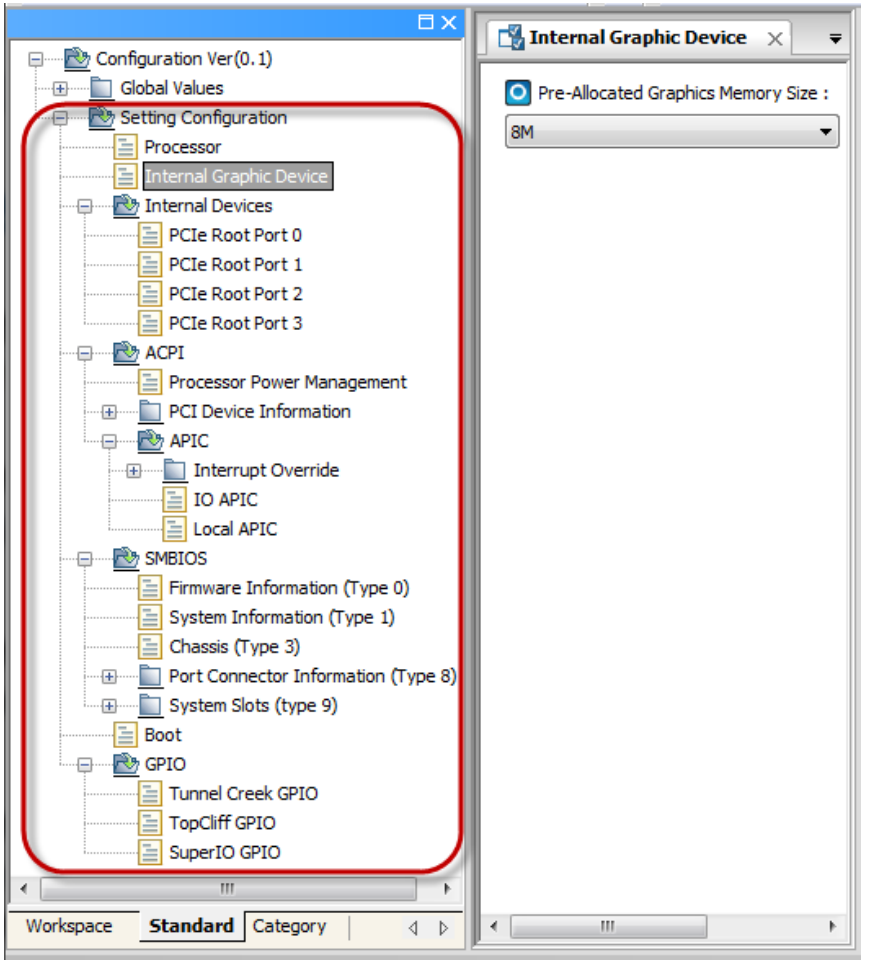
Intel® BLDK is targeted at fixed-function devices. It does not replace need for full-featured BIOS.

Agenda

- Introduction to the Intel® Boot Loader Development Kit (Intel® BLDK)
- Features and Capabilities of Intel BLDK
- **Firmware Customization and Optimization**
- Debugging with Intel BLDK
- Q & A

Firmware Customization

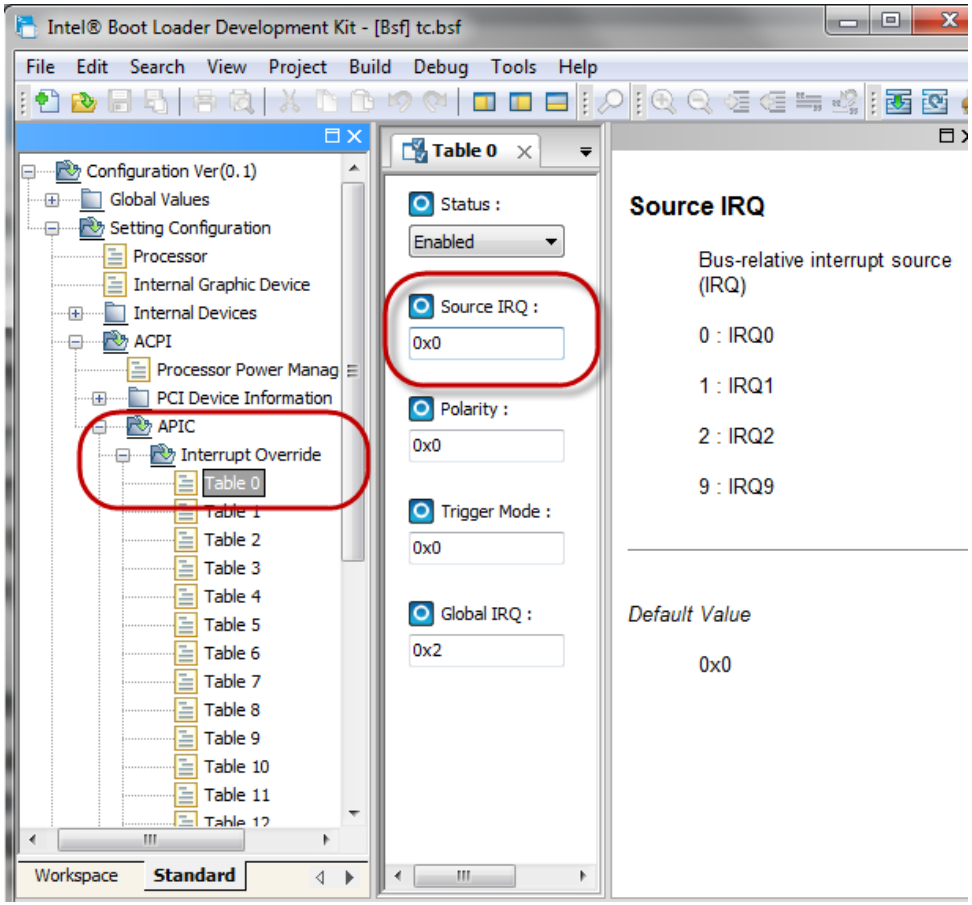
- Development Application provides the ability to customize firmware
- Hundreds of firmware options are configurable through the Development Application
- No source modification is required



Intel® BLDK provides an easy-to-use firmware configuration solution

Binary Modification

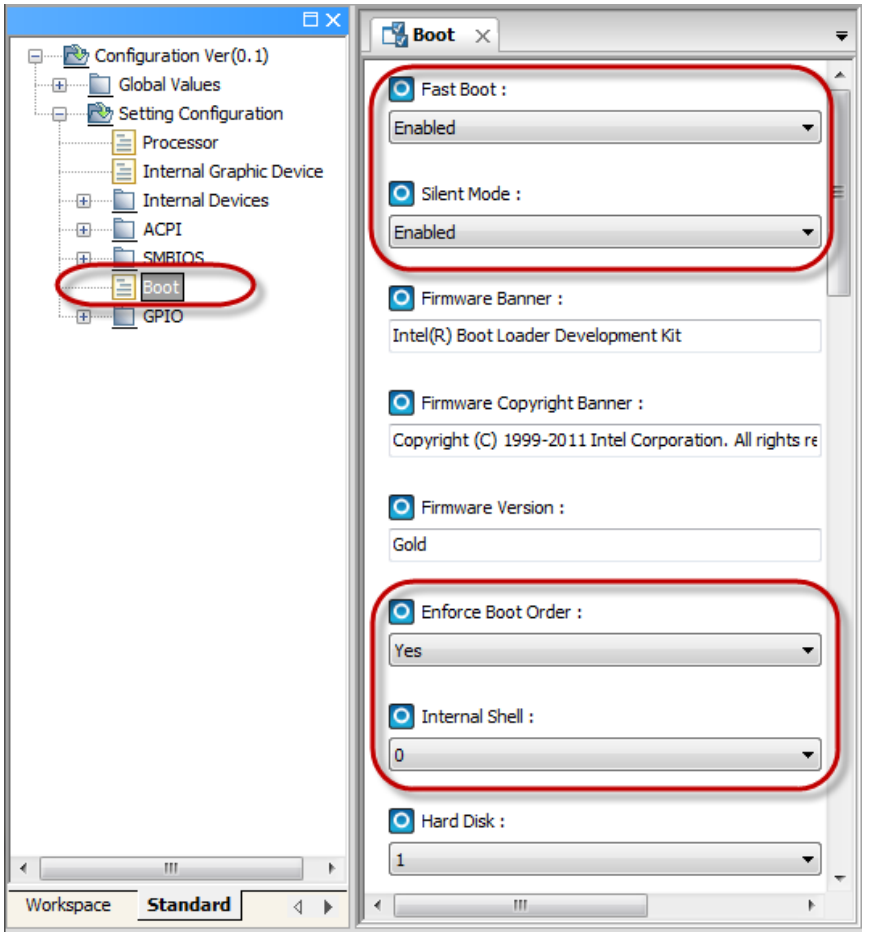
- Provides board customization and porting without rebuilding image or source code updates
- Post-build firmware configurations are accessed through Intel® BLDK Development Application
- 3-Step Process:
  1. Create a project
  2. Modify parameters based on the Target Configuration using Development Application
  3. Generate binary image



Intel® BLDK provides support for simple binary configuration

Performance Optimization in Intel® BLDK

- Intel® BLDK boot sequence can be configured for fast boot via the Development Application
- Only drivers required for system boot are dispatched
- Faster boot times can be achieved by optimizing Intel BLDK for a specific target configuration
  - Download "Reducing Platform Boot Time in UDK2010" for further details

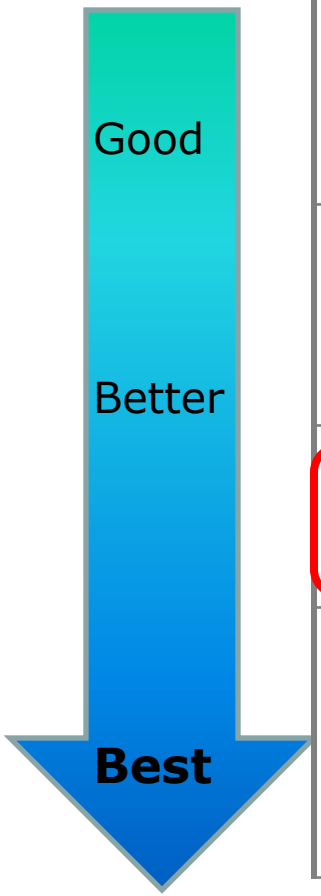


Intel® BLDK is optimized for fast boot

Agenda

- Introduction to the Intel® Boot Loader Development Kit (Intel® BLDK)
- Features and Capabilities of Intel BLDK
- Firmware Customization and Optimization
- **Debugging with Intel BLDK**
- Q & A

Platform Debug Methodologies



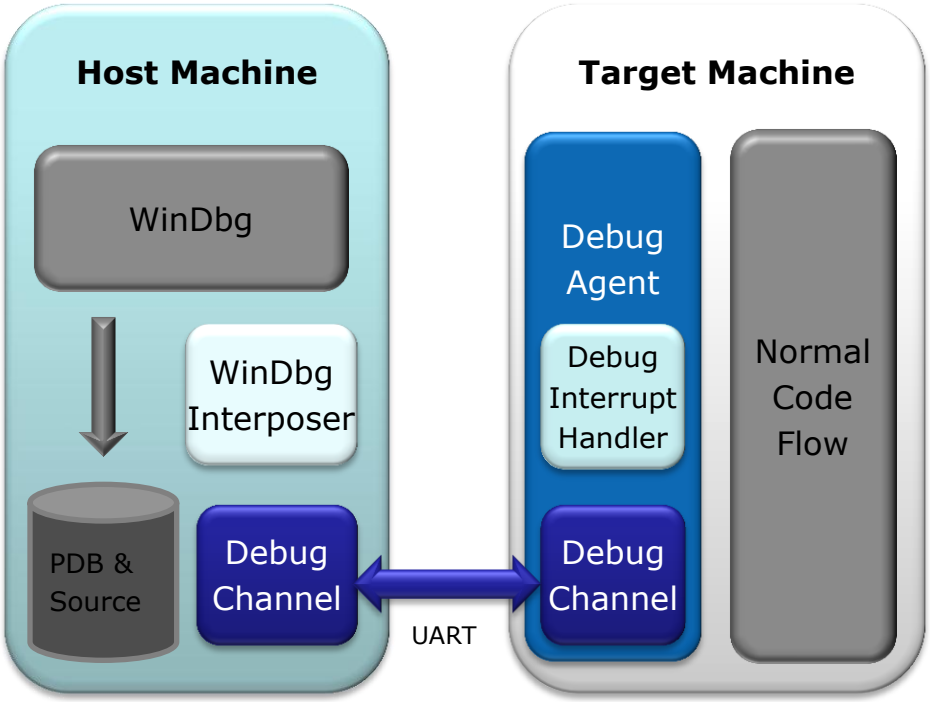
Method	Pros	Cons
Port 80h	• Simple • Low overhead	• Limited information • No execution tracing / flow control • May require several build iterations to isolate failure
Serial Out	• Simple • Low overhead • More information than Port 80h	• Additional hardware and initialization • No execution tracing / flow control
Software Debugger	• Freely available • Source level debug • Execution tracing / flow control	• Debug agent on target • Cannot debug all flows
Hardware Debugger	• Source level debug • Ability to step through code • Greater visibility to HW • Ability to debug complex execution paths (CPU init, SMM)	• Requires purchase of JTAG debugger

Software Debugger is integrated with Intel® BLDK

Intel® BLDK - Debugging

Intel BLDK includes a software debug solution

- WinDbg Interposer interprets the commands from WinDbg
- Debug channels are in charge of communication between Host Machine and Target Machine
- Debug interrupt handler handles the commands from Debug channel



For more details about the Intel UDK Debugger Tool, please refer to:
http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=EDK2

Hardware debug solutions is available from:

Macraigor Systems Complete JTAG Debug Support

Arium

WIND RIVER

intel Embedded

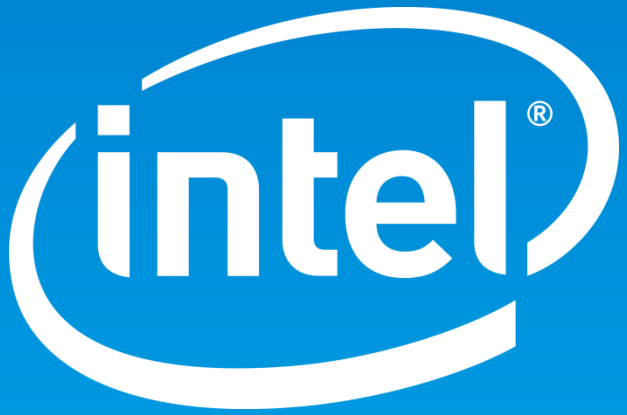
Summary

- **Intel® BLDK is a royalty-free solution for fixed-function embedded devices**
- **Intel BLDK is a complete solution that includes source, binaries, debug tools and documentation**
- **Intel BLDK reference implementations available now for:**
  - **Intel® Atom™ Processor E6xx Series**
  - **Intel® Atom™ Processor E6x5C Series**
  - **Coming Soon:**
    Intel® Atom™ Processor N2000 and D2000 Series

Call to Action

- ***Attend our hands-on Lab at 10:30 or 2:00!***
- **Download Intel® BLDK and related whitepapers and documentation (http://www.intel.com/go/bldk)**
- **Experiment with Intel® BLDK on your Intel reference platform**
- **Identify 3rd parties that can assist with development efforts (http://www.intel.com/go/eca)**
- **Visit the online community support forum (http://edc.intel.com/community)**

Q & A


intel

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.
- 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 processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number
- Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel representative to obtain Intel's current plan of record product roadmaps.
- Intel, Intel Atom, Intel vPro, 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.
-

intel Embedded

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. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should,” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. 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 company’s expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions, including supply constraints and other disruptions affecting customers; 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. Potential disruptions in the high technology supply chain resulting from the recent disaster in Japan could cause customer demand to be different from Intel’s expectations. 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 affected 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 April 2, 2011.

Rev. 5/9/11